eHealth Ontario
www.ehealthontario.on.ca

Service Interaction Guide

Incident, Problem, and Change Management

Version: 3

Date: November 7, 2017

Document ID: 4164

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Document Control

The electronic version of this document is recognized as the only valid version.

Document Sensitivity Level

Information that is generally available to eHealth Ontario staff, consultants, vendors, and approved non-eHealth Ontario workers. A breach of such information would cause minimal impact.

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE
3	2017-11-07	Quarterly Review Re-publication - based on updates to Privacy Flows as per addition of ServiceOntario and MOHLTC Access & Privacy Office contact points, as appropriate, in consultation with Ministry personnel and eHealth Ontario Privacy Office
2	2016-09-30	Quarterly Review Re-Publication - Correction to hours of operation for eHealth Ontario Business Desk; added requirement for service owner approval for changes to the Regular Maintenance Window; format fixes. Based on draft version 1.01_20160930
1	2016-02-19	First standard Service Interaction Guide, based on draft version 0.03

Table of Contents

List of Figures

List of Tables

1.0 Introduction

1.1 Document Purpose

The purpose of the Service Interaction Guide is to ensure proper communication between organizations with respect to incident management, problem management, and change management of eHealth Ontario services so that the interaction points between eHealth Ontario and a partnering organization can be understood, adopted, and socialized with the partnering organization. This document outlines the eHealth Ontario standards for interaction between eHealth Ontario and a partnering organization across the business and technical eHealth Ontario demarcation, and during the operational life of an eHealth Ontario service. Specific activities of the eHealth Ontario Incident, Problem, and Change Management Process are, within the context of the partnering organization's role, outlined in order to effectively troubleshoot incidents, fulfill service requests, avoid persistent problems and undesired incident trending, and effectively manage changes to the live environment of the service.

1.2 Scope

Aspects of the Incident, Problem, and Change Management processes internal to eHealth Ontario are not documented here. Adoption of this guide does not imply review or approval of eHealth Ontario internal processes. This document outlines the eHealth Ontario standard touchpoints with partnering organizations such that the processes can be utilized seamlessly from end to end of the support chain.

1.3 Audience

This document is intended for the Incident, Problem, and Change Management teams of any of the following types of external organizations who enter into a direct relationship with eHealth Ontario in a business and/or technical capacity to enable the successful performance of an eHealth Ontario service, herein after referred to as 'the partnering organization:'

- Delivery Partners
- Service Providers
- Clients
- Customers
- Vendors[1]

It is also intended for use by eHealth Ontario's Client Services and Service Delivery personnel who are responsible for responding to service requests, incidents, and inquiries related to incidents.

[1] Vendor relationships between eHealth Ontario and third party vendors are governed by the current contracts agreed to between eHealth Ontario and the vendor. Any agreed terms, means of contact with eHealth Ontario, and SLAs or SLOs contained therein supersede any of the touchpoints and terms set out in the *eHealth Ontario Service Interaction Guide*.

Partnering organizations with direct relationships to third party service providers or third party vendors that participate in the support chain of any eHealth Ontario service are responsible to convey the eHealth Ontario standards contained in this guide with their third party service providers and third party vendors.

Note: The eHealth Ontario Service Interaction Guide is subject to Change Management. It is considered to be a Configuration Item and is owned by eHealth Ontario.

2.0 Incident Management

The information in this section is used to baseline interactions of a partnering organization with eHealth Ontario for the purposes of incident management. The Incident Management process at eHealth Ontario follows the Information Technology Infrastructure Library (ITIL), V3 best practice. Incident Management is the repeatable process used by eHealth Ontario to help restore normal service as quickly as possible with minimal disruption to the business. This ensures that the best achievable levels of availability and service are maintained, as expected, within eHealth Ontario Standard Service Level Targets.

To ensure proper communication between organizations with respect to incident management, this section outlines the integration points with a partnering organization and how they will be engaged when needed to assist with eHealth Ontario Incident Management activities, and vice versa.

2.1 Service Desks

2.1.1 eHealth Ontario Service Desk

The eHealth Ontario Service Desk is made up of a Service Desk and a Business Desk. The eHealth Ontario Service Desk is the point of contact/interface for incident reporting and service request purposes. It is responsible for the recording and life-cycle management of all incidents that affect the operational service delivered to clients, including coordination of technical support in the operation groups, and use and implementation of eHealth Ontario infrastructure products and services pertaining to any eHealth Ontario service.

The eHealth Ontario Service Desk accepts calls reporting high priority incidents (priority 1 and 2) and low priority incidents (priority 3 and 4) pertaining to the degraded performance of any eHealth Ontario service, and all service requests pertaining to any eHealth Ontario service.

This can include any of the following external parties:

- End users
- Patients or substitute decision makers
- External technical teams
- External Tier 1 support desks
- Local support desks

- Support desks of partnering organizations
- Local Registration Agents (LRA)
- Express Registration Agents (ERA)
- External privacy officers
- External security officers
- Vendor support desks
- Service Ontario
- Ministry of Health and Long-term Care Access and Privacy Office
- Ontario Public Drug Programs (OPDP)
- Information Management Strategy and Policy Branch (IMSP)

The eHealth Ontario Service Desk contact information is:

Contact Information	Email:* servicedesk@ehealthontario.on.ca Phone:* 1-866-250-1554 Fax: 416-586-4040 (Please phone the eHealth Ontario Service Desk to notify them when faxing any information related to an incident or service request.) **Note: Phone is the primary method of contact for the eHealth Ontario Service Desk. There is currently no Service Level Agreements (SLAs) for incidents or service requests opened at the eHealth Ontario Service Desk via email. Rather, there are Service Level Objectives (SLOs). See the Service Levels section of this document for details.*
Hours of Operation	**Service Desk**: Call to report all incidents to the eHealth Ontario Service Desk - 7/24/365. **Business Desk**: 8:00 a.m. to 5:00 p.m., Eastern Standard Time (EST)

The eHealth Ontario Business Desk has fail-over support provided by the eHealth Ontario Service Desk after business hours.

2.1.2 Partnering Organization Service Desk

Partnering organizations are to contact the eHealth Ontario Service Desk once initial investigations are completed by the partnering organization and the source of the issue is identified as being related to the services provided by eHealth Ontario.

Contact details of the partnering organization’s service desk are to be provided during the project phase of the service. Any changes to the contact details during the operational life of the service are to be reported to the eHealth Ontario Service Desk, which are then conveyed as a service request to the assigned eHealth Ontario Service Manager.

Escalation points and off-hours contacts for the partnering organization need to be established for the duration of the service operational life, and provided to the assigned Service Manager for the eHealth Ontario service. These contacts will be used for clarification on priority levels, issues with troubleshooting measures during resolution, follow up on expedient resolution of high priority incidents, as well as follow up on the performance of the partnering organization's service desk and its adherence to eHealth Ontario standard support flows.

2.2 Incident Priority and Service Level Targets

An incident is any event which is not part of the standard operation of a service and which causes, or may cause an interruption to, or a reduction in, the quality of that service performance. Priority is used to identify the relative importance of an incident based on impact and urgency, which establishes the SLA for the ticket. eHealth Ontario follows its standard Incident Management process to categorize and prioritize incidents for eHealth Ontario services.

eHealth Ontario standards for incidents are priority levels 1 to 4, and based on the criticality of the service and number of users/sites impacted by the incident, i.e., impact and urgency:

- Priority 1 and 2 incidents are supported for resolution 24/7/365
- Priority 3 and 4 incidents are supported during eHealth Ontario business hours, 8:00 a.m. to 5:00 p.m., Eastern Standard Time (EST)

In the event that the service desk of a partnering organization that owns or manages components that enable the overall successful performance of an eHealth Ontario service, along with the support groups affiliated with those components, does not align with the hours of operation provided by eHealth Ontario (i.e., 7/24/365 for major incidents), the eHealth Ontario standard SLAs may not be achievable for that service.

All incidents should be reported to the eHealth Ontario Service Desk by phone which will start priority assignment, investigation, and resolution of the incident.

Automatic updates on incident status are provided to the reporting party by email through eHealth Ontario's ticketing system. Updates are provided when the incident is placed in the following statuses: *In Progress*, *Pending*, and *Resolved*.

See **Appendix B** for the outline of the eHealth Ontario standard priority levels and service level targets for incidents.

2.3 Service Request Priority and Service Level Targets

A Service Request is a question, inquiry, complaint, or request for assistance related to eHealth Ontario support services. Fulfillment of the service request supports the performance of an eHealth Ontario service in meeting its SLAs indirectly, e.g., password resets on a technical administrator account.

eHealth Ontario standards for service requests are priority levels 1 to 4. All service requests are supported during eHealth Ontario business hours, 8:00 a.m. to 5:00 p.m., EST.

All Service Requests should be directed to the eHealth Ontario Service Desk.

See **Appendix C** for the outline of the eHealth Ontario standard priority levels and service level targets for service requests.

2.4 Ticket Classification

Incident priority definitions are outlined in the Service Provider Agreement that is completed during the project phase of the eHealth Ontario service lifecycle.

2.4.1 Normal Incidents

A ticket can be opened in one of the following ways:

1. Upon receiving a call from the partnering organization service desk reporting an incident or a service request related to the business or technical domain of eHealth Ontario as it pertains to the eHealth Ontario service, the eHealth Ontario Service Desk will create a ticket.
2. Upon receiving an alert from a monitoring system, the eHealth Ontario Support Group responsible for receiving event alerts will create a ticket and assign it to another eHealth Ontario Support Group(s) to action.
3. Upon receiving an email message from the partnering organization service desk reporting an incident or a service request related to the business or technical domain of eHealth Ontario as it pertains to the eHealth Ontario service, the eHealth Ontario Service Desk will create a ticket.[2]

The completed eHealth Ontario ticket will contain detailed incident ticketing information as specified in the 'Ticket Assignment' section of this document. See below.

Upon opening a normal ticket, the operational support teams of the partnering organization may be requested to collaborate with eHealth Ontario support teams via eHealth Ontario hosted conference bridges.

2.4.2 Major Incidents

eHealth Ontario invokes a Major Incident Process when any critical service is determined to be unavailable or degraded to the point where unusable. Major Incidents are classified as either P1-Critical or P2-High.

eHealth Ontario will assign an Incident Coordinator to co-ordinate the major incident to resolution via tele-conference bridge and WebEx as necessary, engaging internal and external support resources, as required. Upon opening a major incident ticket, the partnering organization support teams and/or those of their vendor may collaborate with eHealth Ontario support teams via the eHealth Ontario hosted conference bridges.

eHealth Ontario will inform partnering organizations and impacted end user sites via the eHealth Ontario Service Desk when incidents affect accessibility and availability of eHealth Ontario services through Service Interruption Notifications. When service is restored, a Service Restoration Notice will be forwarded to the

[2] There are no SLAs attached to tickets initiated via email.

same partnering organizations and end users as required. These are also known within eHealth Ontario as *unplanned outages*.

2.4.2.1 Major Incident Review

Following a major incident, eHealth Ontario will conduct a Major Incident Review (MIR) and, if required a Root Cause Analysis (RCA) session to identify and correct any process and/or technical design gaps. eHealth Ontario Incident Management will schedule the major incident review within two business days of the incident (target) and finalize the Major Incident Report within five business days (target). In most cases, the partnering organization can receive a copy of the major incident report if requested.

The major incident findings will also be reviewed as part of a regular scheduled service review meeting which is a part of the eHealth Ontario Incident Management process.

> **Note:** eHealth Ontario reserves the right to exclude sensitive information (IP Addressing, server names etc.) from the major incident report as required to ensure security and integrity of its EHR systems.

2.4.3 Security Incidents

eHealth Ontario provides leadership in management of security incidents pertaining to services owned and managed by eHealth Ontario. In the event a security incident detected by eHealth Ontario, reported by the partnering organization, or any other third party, the eHealth Ontario Service Desk will create a ticket and the eHealth Ontario Security Incident Response (SIR) process will be initiated.

The eHealth Ontario Service Desk will inform the partnering organization via their service desk of security incidents and the resolution thereof.

The partnering organization will inform eHealth Ontario via the eHealth Ontario Service Desk of security incidents not related to the eHealth Ontario business and technical domain of support, and the resolution thereof.

2.4.4 Privacy Incidents/Breach

Privacy Incidents are handled differently depending on the service involved and whether the actor is a member of the general public (patient, substitute decision maker, or other), an end user (clinician), or a Local Privacy Officer.

A possible Privacy Incident reported by the general public or by end users is treated as a Privacy Operations Request (a privacy complaint) until it is validated by an appropriate party, i.e., a Local Privacy Officer, a trained clinician. As such, the general public reports suspected privacy incidents to clinicians (end users), and end users report privacy breaches or suspected privacy incidents to eHealth Ontario via a Local Privacy Officer. Local Privacy Officers utilize eHealth Ontario as the tier 1 support level for all privacy incidents and breaches. Privacy incidents and breaches are to be reported to eHealth Ontario via the eHealth Ontario Service Desk. The eHealth Ontario Service Desk will create a ticket and the eHealth Ontario Privacy Incident and Breach Management (PBM) process is initiated. See figures 2 and 3 for high-level privacy operations and privacy incident and breach management support flows.

For end users that are not formally trained in Privacy Breach Awareness, privacy complaints submitted to eHealth Ontario by the end user directly or on behalf of a patient must be validated by a Local Privacy Officer, where one is established.

Where there is no Local Privacy Officer at a site, and where the privacy inquiry or complaint relates to ConnectingOntario (cOntario) and Diagnostic Images (DI) Services, the general public submits inquiries or complaints directly to eHealth Ontario via its service desk which may then be validated and categorized by the eHealth Ontario Privacy Office as a privacy incident or breach, and which would trigger initiation of the eHealth Ontario Privacy Incident and Breach Management (PBM) process. See figures 2 for high-level privacy operations and privacy incident and breach management support flows.

The general public uses ServiceOntario as the first point of contact to submit a privacy inquiry or complaint for DHDR and DPV services. As such, any privacy inquiry or complaint that is validated and investigated by the appropriate Ministry Program area (OPDP) is directed to eHealth Ontario via its Service Desk for confirmation of a privacy incident or breach. See figure 2 for high-level privacy operations and privacy incident and breach management support flows.

The general public uses the Ministry of Health and Long-term Care (MOHLTC) Access & Privacy Office (APO) as the first point of contact to submit a privacy complaint for the OLIS service. As such, any privacy complaint that is validated and investigated by the appropriate Ministry Program area (IMSP), is directed to eHealth Ontario via its Service Desk for confirmation of a privacy incident or breach. See figure 2 for high-level privacy operations and privacy incident and breach management support flows.

Privacy Incidents directed to eHealth Ontario Service Desk should not contain personal information (PI) or personal health information (PHI). At any time during the course of engagement with the eHealth Ontario Privacy Office during privacy incident and breach management PI or PHI needs to be exchanged between eHealth Ontario and a partnering organization, and where there is no way around ticket resolution otherwise, the eHealth Ontario standard modes of electronic delivery are as follows:

1. Email: Depending on whether the partnering organization uses eHealth Ontario ONE Mail®, as follows:

    a. If the organization is an eHealth Ontario ONE Mail subscriber, send information to privacy.operations@ehealthontario.on.ca using the ONE Mail account

    b. If the organization is not an eHealth Ontario ONE Mail subscriber: password protected, zipped, and encrypted documents attached to email

2. Phone: Call eHealth Ontario Privacy Office directly at 416-946-4767

3. Secure Fax: Fax information to 416-586-4397 (eHealth Ontario Business Desk Fax Service)

The partnering organization is to provide tier 2 level support for Privacy Incident and Breach Management as follows (and as applicable for that organization's domain of support):

- Investigation as a result of a complaint
- Contain Incident/Breach
- Notify impacted individuals

- Cooperate during Breach Investigation
- Act as Breach Investigation Lead, where eHealth Ontario has determined this as the appropriate procedure
- Remediate Incident/Breach

2.4.5 Privacy Operations Requests

Privacy Operations requests include any of the following:

- block or unblock patient records (i.e., consent directive)
- report of patient records
- audit report of access to patient records, including consent directive history reports
- audit report for a privacy officer
- correction to clinical data in a patient record
- privacy inquiry
- privacy complaint[3]

Privacy operations requests are handled differently depending on the service involved and whether the actor making the request is the general public, an end user, or a Local Privacy Officer.

For privacy operations requests from the general public for ConnectingOntario and DI services, eHealth Ontario Service Desk is the first point of contact.[4] eHealth Ontario fulfills the privacy operations request, investigates inquiries/complaints and, upon categorization and validation of a privacy incident, engages the Privacy Breach Management (PBM) process, as appropriate, and/or engages partnering organizations to carry out underpinning request fulfillment or breach management collaborative actions, as appropriate. See figure 2 for high-level privacy operations and privacy incident and breach management support flows.

For privacy operations requests from the general public for the DHDR service, the DPV service, and consent directive requests for the OLIS service, ServiceOntario is the first point of contact. ServiceOntario carries out underpinning actions for OLIS consent directives and assigns completion of the request to the eHealth Ontario Privacy Office. For DHDR access report requests (including requests for consent directive history reports), inquiries or complaints, ServiceOntario assigns these to the Ministry Program, OPDP; OPDP fulfills underpinning actions for these access requests and engages the eHealth Ontario DHDR Business Support team directly for completion. For DPV access report requests (including requests for consent directive history reports), inquiries or complaints, ServiceOntario assigns these to the Ministry Program, OPDP; OPDP fulfills underpinning actions for these access requests and engages the Ministry's Health Services Cluster

[3] The eHealth Ontario Service Desk assigns the Privacy Operations request directly to the eHealth Ontario Privacy Office when inquiries/complaints have been validated and investigated by either the Local Privacy Officer or the Ministry Program Area. These inquiries/complaints are treated as suspected privacy incidents or breaches until they are validated by the eHealth Ontario Privacy Office.

[4] ConnectingOntario provides clinical access to DHDR and OLIS data. As such, privacy requests or concerns related to DHDR and OLIS that arise through experience with the ConnectingOntario service shall follow the support channel outlined for those services respectively (as outlined here).

(HSC) directly for completion. If the request is for PHI/PI correction, ServiceOntario redirects the requestor to the point of data entry (either a Service Ontario local office, the healthcare practitioner, or the pharmacy) in order to have that correction carried out at the data source. OPDP investigates inquiries and complaints and, if any are validated as a privacy incident, the eHealth Ontario PBM process is initiated by reporting it to the eHealth Ontario Service Desk. See figure 2 for high-level privacy operations and privacy incident and breach management support flows.

For all other privacy operations requests from the general public pertaining to the OLIS service, the Ministry of Health and Long-term Care (MOHLTC) Access & Privacy Office (APO) is the first point of contact. MOHLTC APO assigns OLIS access report requests (including consent directive history reports), inquiries or complaints to the Ministry Program, IMSP; IMSP fulfills underpinning actions for these requests and engages the eHealth Ontario Privacy Office directly for completion. If the request is for PHI/PI correction, the MOHLTC APO redirects the requestor to the point of data entry (either a Service Ontario local office, the healthcare practitioner, or the laboratory) in order to have that correction carried out at the data source. IMSP investigates inquiries and complaints and, if they are validated as a privacy incident, the eHealth Ontario PBM process is initiated by reporting it to the eHealth Ontario Service Desk. See figure 2 for high-level privacy operations and privacy incident and breach management support flows.

For privacy operations requests initiated by a Local Privacy Officer on behalf for him/herself, on behalf of a patient, or on behalf of an end user, the Local Privacy Officer utilizes eHealth Ontario Service Desk as the first point of contact. eHealth Ontario then engages partnering organizations to carry out underpinning actions or collaborate in the PBM process, as appropriate. See figure 3 for details related to support flows with the Local Privacy Officer interacting with eHealth Ontario.

Note: Privacy inquiries and complaints reported to other contact points are considered privacy operations requests until they are validated as privacy incidents/breaches, after which eHealth Ontario Service Desk is the first point of contact for all services for reporting of any Privacy Incident or Breach, as indicated in the previous section.

Privacy Operations requests directed to eHealth Ontario Service Desk should not contain personal information (PI) or personal health information (PHI).

The partnering organization may be requested by the eHealth Ontario Privacy Office to provide more information, as required.

The Local Privacy Officer at a partnering organization has the capacity to directly fulfill a number of requests:

- Consent Directive on behalf of the patient
- Access Request if it relates to only their records, including Consent Directive History reports (see figure 4)
- Correction Request
- Inquiry, if it is related to only their organization or where they may otherwise be able to respond
- Complaint, if it is related to only their organization or where they may otherwise be able to respond

At any time during the course of engagement with the eHealth Ontario Privacy Office in relation to a privacy operations request, PI or PHI needs to be exchanged between eHealth Ontario and the partnering organization, and where there is no way to fulfill the request otherwise, the eHealth Ontario standard modes of electronic delivery are as follows:

1. Email: Depending on whether the partnering organization uses eHealth Ontario ONE Mail®, as follows:

    a. If the organization is an eHealth Ontario ONE Mail subscriber, send information to privacy.operations@ehealthontario.on.ca using the ONE Mail account

    b. If the organization is not an eHealth Ontario ONE Mail subscriber: password protected, zipped, and encrypted documents attached to email

2. Phone: Call eHealth Ontario Privacy Office directly at 416-946-4767

3. Secure Fax: Fax information to 416-586-4397 addressed to ‘eHealth Ontario Business Desk Fax Service’

2.4.6 Consent Directive Override Feature & Consent Directive Override Reports

The consent directive (CD) override feature involves direct interaction between the end user and a Viewer interface. When the feature is deployed by the end user, the Viewer then carries out a ‘push’ of information to the Enterprise Reporting System (ERS) application.[5] The ERS application sends an automated notification to either the eHealth Ontario Privacy Office or ServiceOntario, depending on the service for which the CD override was entered (see figure 4). The responsible party to send a letter to the impacted patient depends on the Service involved, as follows:

- ConnectingOntario & DI Viewer – eHealth Ontario Privacy Office sends a letter to the Local Privacy Officer; Local Privacy Officer sends a letter to the patient
- OLIS - eHealth Ontario Privacy Office sends a letter to the patient
- DHDR/DPV – ServiceOntario sends a letter to the patient

For the DHDR Service, Local Privacy Officers utilize a self-serve area in the ERS application to review CD override reports. During review of these reports, the Local Privacy Officer may initiate the PBM process by reporting their validation of a privacy incident to the eHealth Ontario Service Desk.

See figure 4 for a depiction of the flows related to CD override entry and reports.

2.5 Ticket Assignment

Each organization will maintain a reference in their incident management reference tool to the other organization’s ticket number.

[5] The ERS application is hosted on the eHealth Ontario portal.

2.5.1 Partnering Organization Service Desk to eHealth Ontario Service Desk

For any incidents related to the eHealth Ontario business and technical domain of support, the partnering organization service desk will contact the eHealth Ontario Service Desk by phone and provide the following information:

- Authorized caller identifying themselves as the service desk and naming the partnering organization
- Partnering organization ticket number
- Description of the impact of the issue to the service
- Description of the impact of the issue to the end user
- Date and time of when issue first appeared
- Priority
- Description of troubleshooting activities that were undertaken by the partnering organization to rule out issues that are part of their business and/or technical domain
- Workaround status
    - record “no-workaround” or the actual workaround (if applicable)

> **Note:** As noted earlier, telephone is the primary route of ticket creation for the eHealth Ontario Service Desk. Incidents reported through email are not tied to SLAs.

2.5.2 eHealth Ontario Support Team to Partnering Organization Service Desk

For any incidents related to the partnering organization’s domain of business or technical support, the eHealth Ontario Service Desk will engage the partnering organization service desk and provide the following information:

- Authorized caller identified as ‘eHealth Ontario <support team>’
- eHealth Ontario ticket number
- Description of the impact of the issue to the service
- Description of the impact of the issue to the end user
- Date and time of when issue first appeared
- Priority
- Work-around status
    - record “no-workaround” or the actual workaround (if applicable)

2.5.3 Communication

2.5.3.1 Communicating with End-users

eHealth Ontario will not contact the end-user directly for technical incidents and requests that are the sole responsibility of the partnering organization. If the end-user attempts to contact eHealth Ontario directly for any status updates or assistance with regard to such incidents, they will be redirected to the service desk of the partnering organization.

eHealth Ontario will communicate directly with end-users for fulfilment of Privacy Operations requests and Privacy Incident and Breach Management investigation, as well as the general public, patients, and other persons or entities that may initiate same, as outlined in the high-level Privacy Operations and Privacy Incident and Breach Management diagram, above. Any callers who initiate such requests or who are reporting a privacy incident or breach via the partnering organization service desk, or other central communication point within the partnering organization, should be redirected to the eHealth Ontario Service Desk.

In some instances, the Privacy Officer of the partnering organization may act as the first point of triage for a Privacy Operations request or reporting of a Privacy Incident/Breach. That Privacy Officer should then inform eHealth Ontario via the eHealth Ontario Service Desk.

2.5.3.2 Status Requests/Updates

eHealth Ontario Support Groups and the service desk of the partnering organization will communicate with each other to provide status updates and reference the appropriate ticket numbers in each other's ticketing tool, and with sufficient regularity in order to successfully meet the agreed SLAs.

2.5.3.3 Ticket Resolution and Closure

eHealth Ontario and the governing body within the partnering organization will communicate with each other to provide closure details, as needed, and reference the appropriate ticket numbers once resolution is confirmed, as follows:

- eHealth Ontario notification of ticket closure will be directed to the partnering organization service desk
- partnering organization notification of ticket closure will be directed to the eHealth Ontario Service Desk

2.6 Integration Process

2.6.1 Support Demarcation

The business and technical demarcation point between eHealth Ontario and a partnering organization is defined as the boundary between the Configuration Items (CIs) of components owned and managed by the partnering organization and eHealth Ontario's service CIs.

2.6.1.1 Monitoring & Level 1 – Technical & Privacy Support Flows

The following diagram depicts the high-level communication of technical incidents between eHealth Ontario and the partnering organization.

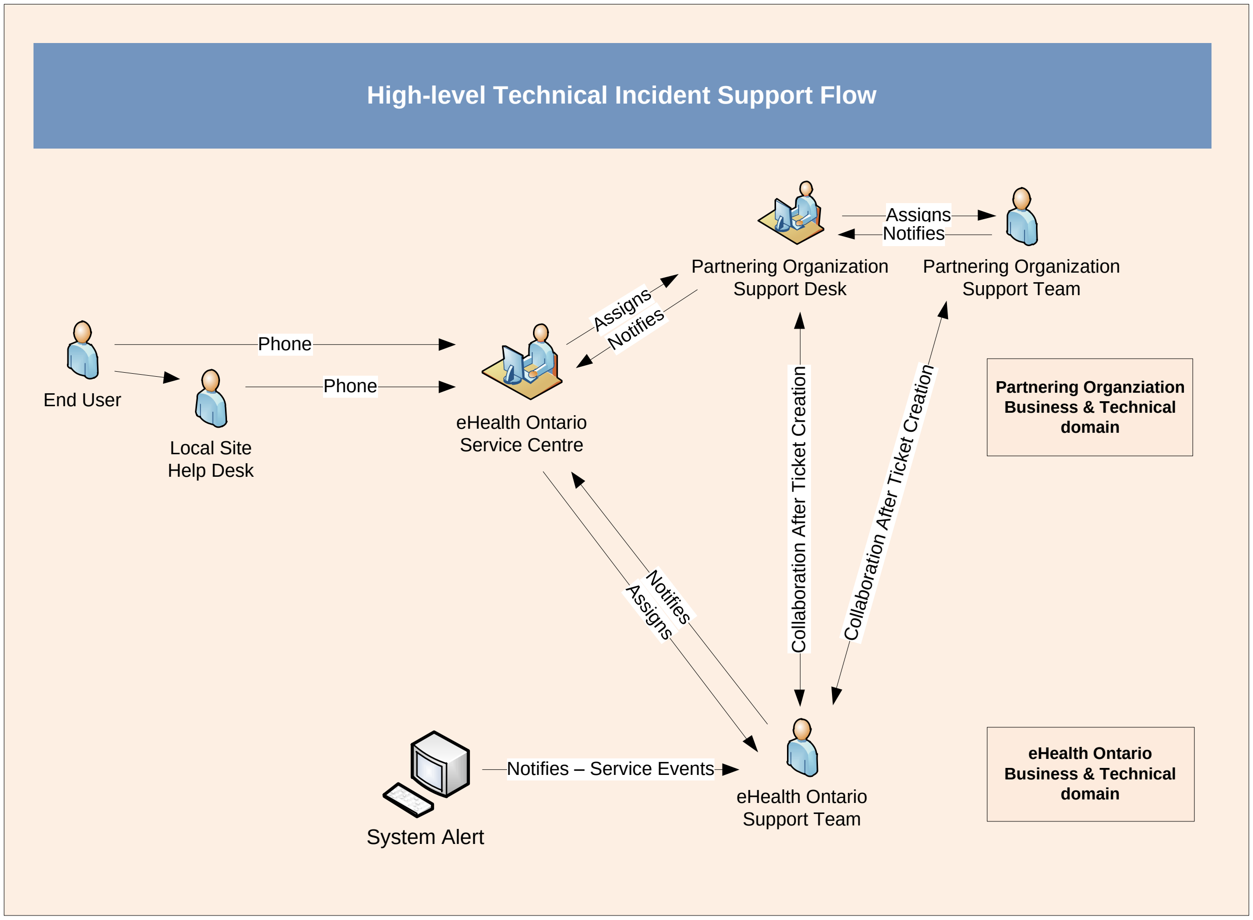
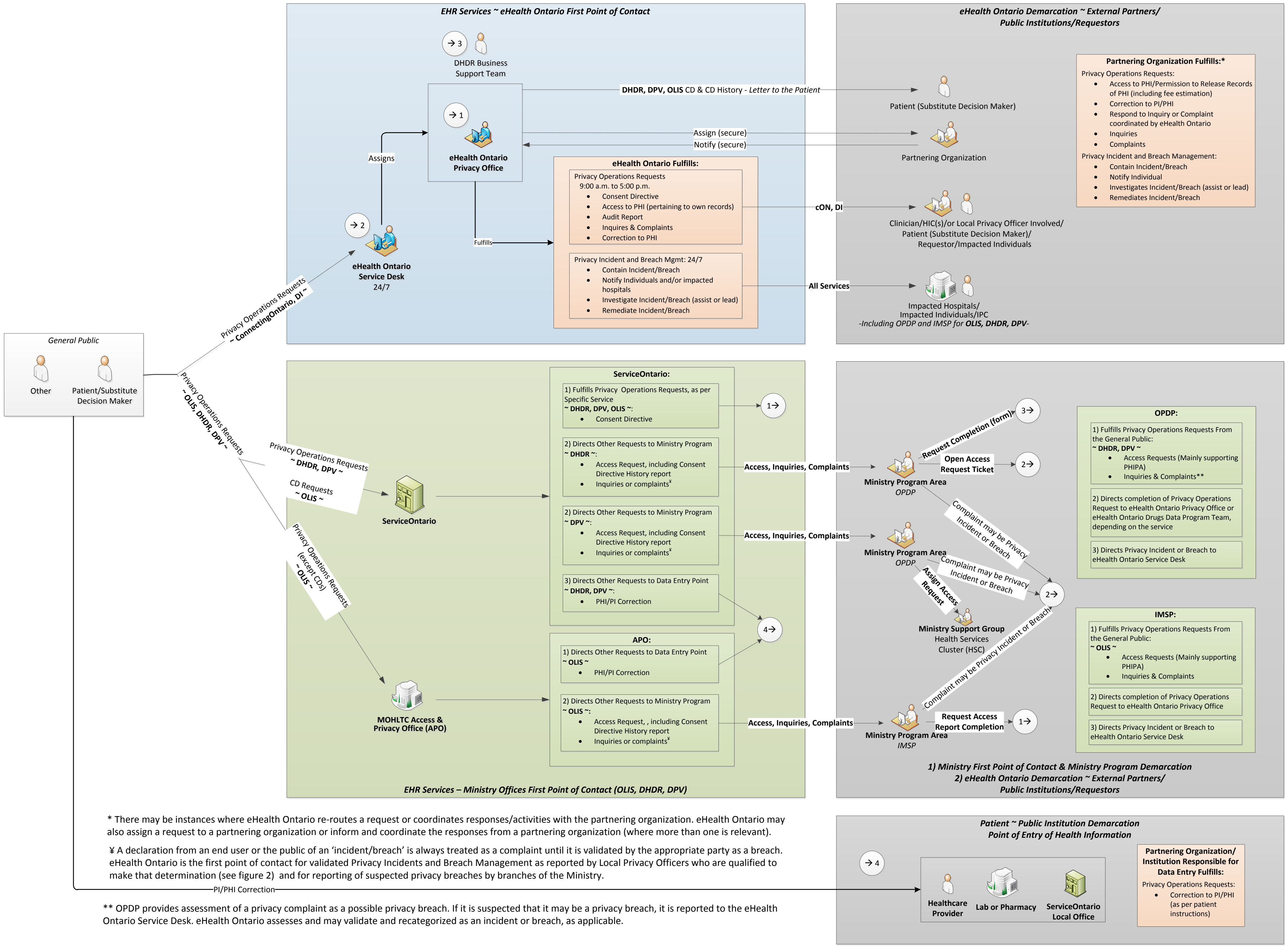

High-level Technical Incident Support Flow
End User
Phone
Local Site Help Desk
Phone
eHealth Ontario Service Centre
Assigns
Notifies
Partnering Organization Support Desk
Assigns
Notifies
Partnering Organization Support Team
Collaboration After Ticket Creation
Collaboration After Ticket Creation
Partnering Organziation Business & Technical domain
Notifies
Assigns
System Alert
Notifies – Service Events
eHealth Ontario Support Team
eHealth Ontario Business & Technical domain

Figure 1 - High-level Technical Incident Support Flow

The following diagram depicts the high-level interactions for Privacy Operations requests and Privacy Incident and Breaches between eHealth Ontario and the partnering organizations where the initiator is the general public.

Privacy Operations Requests (Actors: General Public - Patient/Substitute Decision Maker or Other)


EHR Services ~ eHealth Ontario First Point of Contact
→ 3
DHDR Business Support Team
→ 1
eHealth Ontario Privacy Office
Assigns
→ 2
eHealth Ontario Service Desk 24/7
Fulfills
eHealth Ontario Fulfills:
Privacy Operations Requests 9:00 a.m. to 5:00 p.m.
• Consent Directive
• Access to PHI (pertaining to own records)
• Audit Report
• Inquires & Complaints
• Correction to PHI
Privacy Incident and Breach Mgmt: 24/7
• Contain Incident/Breach
• Notify Individuals and/or impacted hospitals
• Investigate Incident/Breach (assist or lead)
• Remediate Incident/Breach
DHDR, DPV, OLIS CD & CD History - Letter to the Patient
Assign (secure)
Notify (secure)
cON, DI
All Services
eHealth Ontario Demarcation ~ External Partners/ Public Institutions/Requestors
Patient (Substitute Decision Maker)
Partnering Organization
Clinician/HIC(s)/or Local Privacy Officer Involved/ Patient (Substitute Decision Maker)/ Requestor/Impacted Individuals
Impacted Hospitals/ Impacted Individuals/IPC -Including OPDP and IMSP for OLIS, DHDR, DPV-
Partnering Organization Fulfills:*
Privacy Operations Requests:
• Access to PHI/Permission to Release Records of PHI (including fee estimation)
• Correction to PI/PHI
• Respond to Inquiry or Complaint coordinated by eHealth Ontario
• Inquiries
• Complaints
Privacy Incident and Breach Management:
• Contain Incident/Breach
• Notify Individual
• Investigates Incident/Breach (assist or lead)
• Remediates Incident/Breach
General Public
Other
Patient/Substitute Decision Maker
Privacy Operations Requests ~ ConnectingOntario, DI ~
Privacy Operations Requests ~ OLIS, DHDR, DPV ~
Privacy Operations Requests ~ DHDR, DPV ~
CD Requests ~ OLIS ~
Privacy Opeations Requests (except CDs) ~ OLIS ~
ServiceOntario
MOHLTC Access & Privacy Office (APO)
ServiceOntario:
1) Fulfills Privacy Operations Requests, as per Specific Service ~ DHDR, DPV, OLIS ~:
• Consent Directive
2) Directs Other Requests to Ministry Program ~ DHDR ~:
• Access Request, including Consent Directive History report
• Inquiries or complaints¥
2) Directs Other Requests to Ministry Program ~ DPV ~:
• Access Request, including Consent Directive History report
• Inquiries or complaints¥
3) Directs Other Requests to Data Entry Point ~ DHDR, DPV ~:
• PHI/PI Correction
APO:
1) Directs Other Requests to Data Entry Point ~ OLIS ~
• PHI/PI Correction
2) Directs Other Requests to Ministry Program ~ OLIS ~:
• Access Request, , including Consent Directive History report
• Inquiries or complaints¥
1→
4→
EHR Services – Ministry Offices First Point of Contact (OLIS, DHDR, DPV)
Access, Inquiries, Complaints
Access, Inquiries, Complaints
Access, Inquiries, Complaints
Request Completion (form)
3→
Open Access Request Ticket
2→
Ministry Program Area OPDP
Complaint may be Privacy Incident or Breach
Ministry Program Area OPDP
Complaint may be Privacy Incident or Breach
Assign Access Request
2→
Ministry Support Group Health Services Cluster (HSC)
Complaint may be Privacy Incident or Breach
Ministry Program Area IMSP
Request Access Report Completion
1→
OPDP:
1) Fulfills Privacy Operations Requests From the General Public: ~ DHDR, DPV ~
• Access Requests (Mainly supporting PHIPA)
• Inquiries & Complaints**
2) Directs completion of Privacy Operations Request to eHealth Ontario Privacy Office or eHealth Ontario Drugs Data Program Team, depending on the service
3) Directs Privacy Incident or Breach to eHealth Ontario Service Desk
IMSP:
1) Fulfills Privacy Operations Requests From the General Public: ~ OLIS ~
• Access Requests (Mainly supporting PHIPA)
• Inquiries & Complaints
2) Directs completion of Privacy Operations Request to eHealth Ontario Privacy Office
3) Directs Privacy Incident or Breach to eHealth Ontario Service Desk
1) Ministry First Point of Contact & Ministry Program Demarcation
2) eHealth Ontario Demarcation ~ External Partners/ Public Institutions/Requestors
PI/PHI Correction
Patient ~ Public Institution Demarcation Point of Entry of Health Information
→ 4
Healthcare Provider
Lab or Pharmacy
ServiceOntario Local Office
Partnering Organization/ Institution Responsible for Data Entry Fulfills:
Privacy Operations Requests:
• Correction to PI/PHI (as per patient instructions)

* There may be instances where eHealth Ontario re-routes a request or coordinates responses/activities with the partnering organization. eHealth Ontario may also assign a request to a partnering organization or inform and coordinate the responses from a partnering organization (where more than one is relevant).

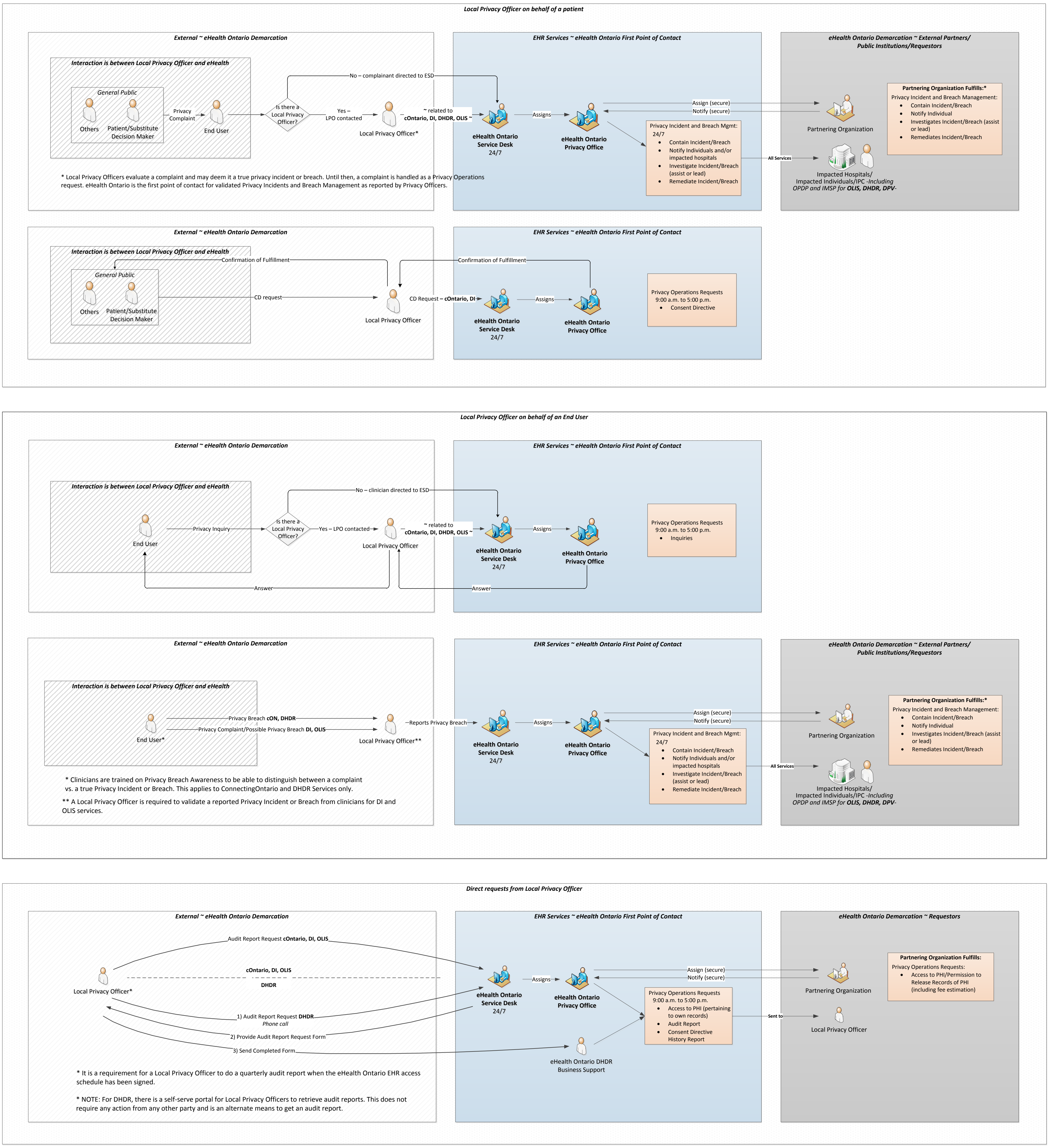
¥ A declaration from an end user or the public of an 'incident/breach' is always treated as a complaint until it is validated by the appropriate party as a breach. eHealth Ontario is the first point of contact for validated Privacy Incidents and Breach Management as reported by Local Privacy Officers who are qualified to make that determination (see figure 2) and for reporting of suspected privacy breaches by branches of the Ministry.

** OPDP provides assessment of a privacy complaint as a possible privacy breach. If it is suspected that it may be a privacy breach, it is reported to the eHealth Ontario Service Desk. eHealth Ontario assesses and may validate and recategorized as an incident or breach, as applicable.

Figure 2 - Privacy Operations & Privacy Incident and Breach Management Support Flow – Actor: General Public

The following diagram depicts the high-level interactions for Privacy Operations requests and Privacy Incident and Breaches between eHealth Ontario and the partnering organizations where the initiator is the Local Privacy Officer.

Privacy Operations Requests – Complaint, Consent Directive (CD), Inquiry – & Privacy Breach Management (Actor: Local Privacy Officer)


Local Privacy Officer on behalf of a patient
External ~ eHealth Ontario Demarcation
Interaction is between Local Privacy Officer and eHealth
General Public
Others
Patient/Substitute Decision Maker
Privacy Complaint
End User
Is there a Local Privacy Officer?
No – complainant directed to ESD
Yes – LPO contacted
Local Privacy Officer*
~ related to cOntario, DI, DHDR, OLIS ~
EHR Services ~ eHealth Ontario First Point of Contact
eHealth Ontario Service Desk 24/7
Assigns
eHealth Ontario Privacy Office
Assign (secure)
Notify (secure)
Privacy Incident and Breach Mgmt: 24/7
Contain Incident/Breach
Notify Individuals and/or impacted hospitals
Investigate Incident/Breach (assist or lead)
Remediate Incident/Breach
All Services
eHealth Ontario Demarcation ~ External Partners/ Public Institutions/Requestors
Partnering Organization
Impacted Hospitals/ Impacted Individuals/IPC -Including OPDP and IMSP for OLIS, DHDR, DPV-
Partnering Organization Fulfills:*
Privacy Incident and Breach Management:
Contain Incident/Breach
Notify Individual
Investigates Incident/Breach (assist or lead)
Remediates Incident/Breach
External ~ eHealth Ontario Demarcation
Interaction is between Local Privacy Officer and eHealth
General Public
Others
Patient/Substitute Decision Maker
CD request
Confirmation of Fulfillment
Local Privacy Officer
CD Request – cOntario, DI
EHR Services ~ eHealth Ontario First Point of Contact
Confirmation of Fulfillment
eHealth Ontario Service Desk 24/7
Assigns
eHealth Ontario Privacy Office
Privacy Operations Requests 9:00 a.m. to 5:00 p.m.
Consent Directive
Local Privacy Officer on behalf of an End User
External ~ eHealth Ontario Demarcation
Interaction is between Local Privacy Officer and eHealth
End User
Privacy Inquiry
Is there a Local Privacy Officer?
No – clinician directed to ESD
Yes – LPO contacted
Local Privacy Officer
~ related to cOntario, DI, DHDR, OLIS ~
Answer
EHR Services ~ eHealth Ontario First Point of Contact
eHealth Ontario Service Desk 24/7
Assigns
eHealth Ontario Privacy Office
Answer
Privacy Operations Requests 9:00 a.m. to 5:00 p.m.
Inquiries
External ~ eHealth Ontario Demarcation
Interaction is between Local Privacy Officer and eHealth
End User*
Privacy Breach cON, DHDR
Privacy Complaint/Possible Privacy Breach DI, OLIS
Local Privacy Officer**
Reports Privacy Breach
EHR Services ~ eHealth Ontario First Point of Contact
eHealth Ontario Service Desk 24/7
Assigns
eHealth Ontario Privacy Office
Assign (secure)
Notify (secure)
Privacy Incident and Breach Mgmt: 24/7
Contain Incident/Breach
Notify Individuals and/or impacted hospitals
Investigate Incident/Breach (assist or lead)
Remediate Incident/Breach
All Services
eHealth Ontario Demarcation ~ External Partners/ Public Institutions/Requestors
Partnering Organization
Impacted Hospitals/ Impacted Individuals/IPC -Including OPDP and IMSP for OLIS, DHDR, DPV-
Partnering Organization Fulfills:*
Privacy Incident and Breach Management:
Contain Incident/Breach
Notify Individual
Investigates Incident/Breach (assist or lead)
Remediates Incident/Breach
Direct requests from Local Privacy Officer
External ~ eHealth Ontario Demarcation
Local Privacy Officer*
Audit Report Request cOntario, DI, OLIS
cOntario, DI, OLIS
DHDR
1) Audit Report Request DHDR
Phone call
2) Provide Audit Report Request Form
3) Send Completed Form
EHR Services ~ eHealth Ontario First Point of Contact
eHealth Ontario Service Desk 24/7
Assigns
eHealth Ontario Privacy Office
Assign (secure)
Notify (secure)
Privacy Operations Requests 9:00 a.m. to 5:00 p.m.
Access to PHI (pertaining to own records)
Audit Report
Consent Directive History Report
eHealth Ontario DHDR Business Support
Sent to
eHealth Ontario Demarcation ~ Requestors
Partnering Organization
Local Privacy Officer
Partnering Organization Fulfills:
Privacy Operations Requests:
Access to PHI/Permission to Release Records of PHI (including fee estimation)

* Local Privacy Officers evaluate a complaint and may deem it a true privacy incident or breach. Until then, a complaint is handled as a Privacy Operations request. eHealth Ontario is the first point of contact for validated Privacy Incidents and Breach Management as reported by Privacy Officers.

* Clinicians are trained on Privacy Breach Awareness to be able to distinguish between a complaint vs. a true Privacy Incident or Breach. This applies to ConnectingOntario and DHDR Services only.

** A Local Privacy Officer is required to validate a reported Privacy Incident or Breach from clinicians for DI and OLIS services.

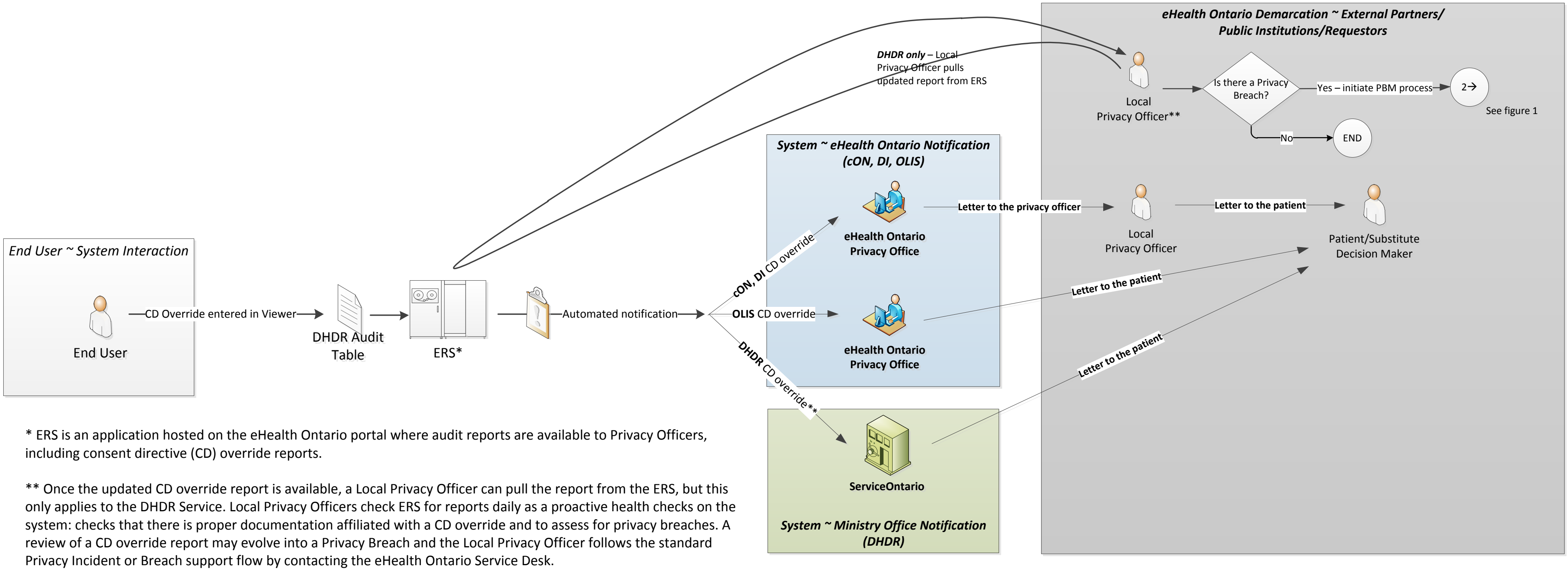
* It is a requirement for a Local Privacy Officer to do a quarterly audit report when the eHealth Ontario EHR access schedule has been signed.

* NOTE: For DHDR, there is a self-serve portal for Local Privacy Officers to retrieve audit reports. This does not require any action from any other party and is an alternate means to get an audit report.

Figure 3 - Privacy Operations & Privacy Incident and Breach Management Support Flows – Actor: Local Privacy Officer

The following diagram depicts the high-level interactions related to the Consent Directive Override feature and access to Consent Direct Override Reports, where the end user and Local Privacy Officer are the proponents triggering the interactions. The PBM process may be initiated by a Local Privacy Officer as a result of review of CD Override Reports after accessing them from the ERS application.

Privacy Operations – Consent Directive (CD) Override Reports (Actors: End User & Local Privacy Officer)



End User ~ System Interaction
End User
CD Override entered in Viewer
DHDR Audit Table
ERS*
Automated notification
DHDR only – Local Privacy Officer pulls updated report from ERS
System ~ eHealth Ontario Notification (cON, DI, OLIS)
cON, DI CD override
eHealth Ontario Privacy Office
OLIS CD override
eHealth Ontario Privacy Office
DHDR CD override**
ServiceOntario
System ~ Ministry Office Notification (DHDR)
Letter to the privacy officer
eHealth Ontario Demarcation ~ External Partners/ Public Institutions/Requestors
Local Privacy Officer**
Is there a Privacy Breach?
Yes – initiate PBM process
2→
See figure 1
No
END
Local Privacy Officer
Letter to the patient
Patient/Substitute Decision Maker
Letter to the patient
Letter to the patient

* ERS is an application hosted on the eHealth Ontario portal where audit reports are available to Privacy Officers, including consent directive (CD) override reports.

** Once the updated CD override report is available, a Local Privacy Officer can pull the report from the ERS, but this only applies to the DHDR Service. Local Privacy Officers check ERS for reports daily as a proactive health checks on the system: checks that there is proper documentation affiliated with a CD override and to assess for privacy breaches. A review of a CD override report may evolve into a Privacy Breach and the Local Privacy Officer follows the standard Privacy Incident or Breach support flow by contacting the eHealth Ontario Service Desk.

Figure 4 - Consent Directive Override Notification and Consent Directive Override Reports – Actor: End User & Local Privacy Officer

2.7 Escalation Touchpoints

Escalation touchpoints at both eHealth Ontario and the partnering organization are used to address any failure point in the incident management support chain in a timely fashion and when meeting the eHealth Ontario standard SLAs for an incident or service request ticket appears to be threatened. Examples include:

- Disagreement regarding a joint service-related decision between the client and eHealth Ontario
- A concern regarding service deployment
- A concern regarding service performance
- A concern regarding the handling of an incident or service request

In the event of an escalation, the partnering organization is to call the eHealth Ontario Service Desk who will in turn engage the Service Manager or Deployment Manager assigned to the eHealth Ontario service. The Service Manager or Deployment Manager, along with the Client Program Manager (if assigned to the eHealth Ontario service), will then act on behalf of the partnering organization to expedite the issue to resolution.

2.7.1 Escalation Touchpoint for eHealth Ontario

eHealth Ontario Service Desk

Phone: 1-866-250-1554
Email address: servicedesk@ehealthontario.on.ca

2.7.2 Escalation Touchpoint for Partnering Organization

The escalation contact point for the partnering organization for engagement in the eHealth Ontario Incident Management process are to be established during the project phase of the service including: role/title, name, email address, mobile/cellular phone, or pager. Any changes to the contact details during the operational life of the service are to be reported to the eHealth Ontario Service Desk, which are then conveyed as a change request to the assigned eHealth Ontario Service Manager for that service.

3.0 Problem Management

3.1 Overview & Introduction

The Problem Management process at eHealth Ontario follows the Information Technology Infrastructure Library (ITIL), V3 best practice. Problem Management at eHealth Ontario is focused on the production environment. A problem is defined as an incident without determination of a root cause upon resolution of the ticket or an undesirable trend observed in a particular configuration item, site, or eHealth Ontario service. A problem can be detected from the eHealth Ontario Incident Management or Change Management processes and can involve any of the incident priority levels.

Problem Management is the process responsible for managing the lifecycle of Problems. Its objective is to prevent Problems and resulting incidents from occurring, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

The Problem Management process is responsible for determining root cause and resolution of Problems using the appropriate control procedures (e.g., Change Management and Release Management). It seeks to identify and maintain information about known errors and work-arounds that can be used by the Support Teams during Incident Management in order to restore service quickly. It is also responsible for the successful correction of any known errors.

Proactive Problem Management is concerned with identifying trends that may reveal potential Problems which allows for the prevention of incidents. Conducting trend analysis of data, including incident records, helps to achieve this.

3.2 Integration Process

3.2.1 Problem Management Process Flow

The following sample diagram identifies the high-level Problem Management process for eHealth Ontario.

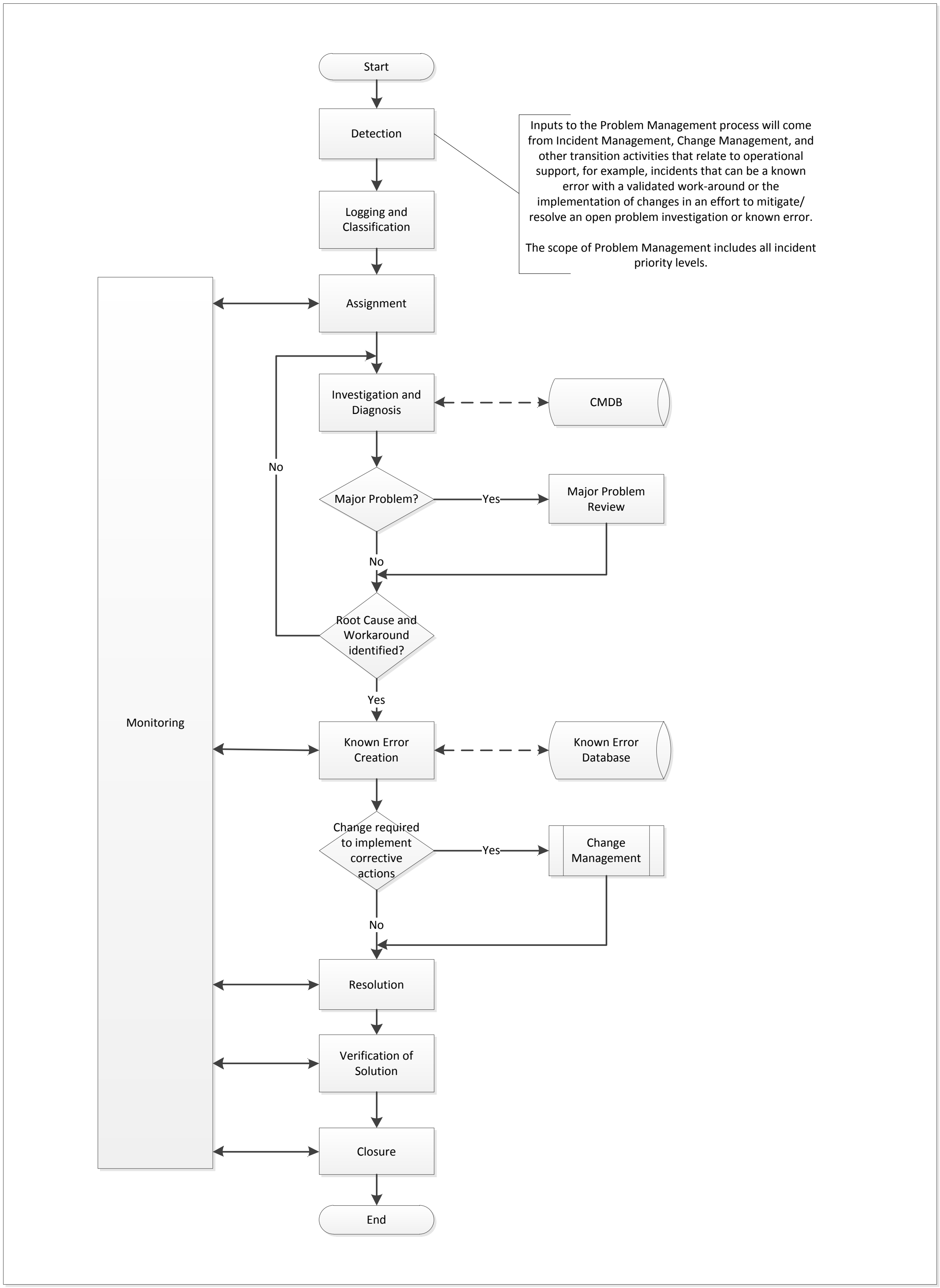

Start
Detection
Inputs to the Problem Management process will come from Incident Management, Change Management, and other transition activities that relate to operational support, for example, incidents that can be a known error with a validated work-around or the implementation of changes in an effort to mitigate/ resolve an open problem investigation or known error.
The scope of Problem Management includes all incident priority levels.
Logging and Classification
Assignment
Monitoring
Investigation and Diagnosis
CMDB
No
Major Problem?
Yes
Major Problem Review
No
Root Cause and Workaround identified?
Yes
Known Error Creation
Known Error Database
Change required to implement corrective actions
Yes
Change Management
No
Resolution
Verification of Solution
Closure
End

Figure 5 - Problem Management Process Flow

3.2.2 Coordination between SPOC Roles in both Organizations

The initiation of problem investigations and other requests regarding problems are to be coordinated via a single point of contact (SPOC) in both eHealth Ontario and the partnering organization, namely, eHealth Ontario Service Manager and Service Manager of a partnering organization (or like role). From this SPOC, ensuing actions and activities will then filter into each organization's internal processes. Likewise, further contact and communications for request of new problem records, problem information, or during other points of investigation will continue to be channeled between the SPOCs.

Once established, contact details for the SPOC must be communicated to the eHealth Ontario Service Manager assigned to that service.

3.2.3 Key Activities and Touchpoints

The following table identifies the high-level key activities/tasks and the touchpoints between a partnering organization and eHealth Ontario in the Problem Management process.

Activity	eHealth Ontario	Partnering Organization
Detection	➢ Review incidents ➢ Analyze incident trends (proactive problem management)	➢ Review incidents ➢ Analyze incident trends (proactive problem management)
Logging and Classification	➢ Create new problem record ➢ Associate incidents to problem record ➢ Notify partnering organization of possible problem ➢ Receive notification of possible problem from partnering organization ➢ Record corresponding problem record in eHealth Ontario Problem Management system ➢ Categorize problem and establish impact, urgency and priority	➢ Create new problem record ➢ Associate incidents to problem record ➢ Notify eHealth Ontario of possible problem ➢ Receive notification of possible problem from eHealth Ontario ➢ Record corresponding problem record in Internal Problem Management system. ➢ Categorize problem and establish impact, urgency and priority
Assignment	➢ Assign to appropriate Problem Analyst ➢ Monitor and track problem	➢ Assign to appropriate Problem Analyst ➢ Monitor and track problem
Investigation and Diagnosis	➢ Conduct problem investigation ➢ Diagnose problem ➢ Document investigation results ➢ Participate in problem investigation and diagnosis, as required ➢ Notify partnering organization of diagnosis with eHealth Ontario originated problem ➢ Provide details on business impact to appropriately guide problem priority ➢ Monitor problem investigation and diagnosis	➢ Conduct problem investigation ➢ Diagnose problem ➢ Document investigation results ➢ Participate in problem investigation and diagnosis, as required ➢ Notify eHealth Ontario of diagnosis with partnering organization originated problem ➢ Provide details on business impact to appropriately guide problem priority ➢ Monitor problem investigation and diagnosis
Resolution	➢ Resolve problem	➢ Resolve problem

Activity	eHealth Ontario	Partnering Organization
Verification of Solution	➢ Verify problem is resolved ➢ Notify partnering organization that the problem is resolved	➢ Verify problem is resolved ➢ Notify eHealth Ontario that the problem is resolved
Closure of Problem	➢ Review problem and analyze if further investigation is required ➢ Notify partnering organization of closure ➢ Receive notification when partnering organization closes a problem ➢ Acknowledge closure of problem record ➢ Close corresponding eHealth Ontario tracking system record, updating relevant information	➢ Review problem and analyze if further investigation is required ➢ Notify eHealth Ontario of closure ➢ Receive notification when eHealth Ontario closes a problem ➢ Acknowledge closure of problem record ➢ Close corresponding partnering organization tracking system record, updating relevant information

Table 1 -High-level Problem Management Key Activities and Touchpoints

3.3 Problem Definition – Standard Problem Information

The following information must be included in all Problem tickets opened by either eHealth Ontario or the partnering organization:

a. Submitter Name and Role
b. Submission Date
c. Description of Problem and Impact
d. Related Incidents or other items
e. Workarounds/Action Plans (if applicable)
f. Recommended Group assignment for investigation

3.4 Problem Triggers

A Problem record can be initiated by either the partnering organization or eHealth Ontario. The Problem Management process is triggered in the following circumstances:

- A major incident occurs where the cause is unknown upon resolution of the incident

- Repeating incidents exhibiting common symptoms or a trend is noticed with a configuration item, lower environment, site, or eHealth Ontario Service (i.e., Proactive Problem Management)

3.5 Problem Review

A review of open problem records is conducted as part of the regular eHealth Ontario/Partner joint monthly meeting. A meeting between Problem Managers can be coordinated through the Service Manager in the partnering organization (or like role) and the eHealth Ontario Service Manager assigned for the relevant service.

A list of problem records is provided to eHealth Ontario by the partnering organization prior to the operational joint monthly meeting. Similarly, eHealth Ontario will provide to the partnering organization a list of service impacting problems related to the eHealth Ontario service. Each organization will represent the components relevant to its technical operations and maintenance responsibility, as explained in the introductory background section, during problem review and investigation meetings. Both the partnering organization and eHealth Ontario will present reports to each other, and eHealth Ontario will lead review and investigation into problems that have an impact to the eHealth Ontario service.

Outside of the Problem Review meeting, ad-hoc updates on problem investigation progress can be requested through the assigned eHealth Ontario Service Manager.

3.5.1 Problem Review Agenda Items

The following items will create the agenda for the problem review meeting:

a. Review open Problem/known error records, confirming their validity, categorization, prioritization and assignment.
b. Discuss each open Problem/known error record, reviewing the latest updates in the problem listing report, progress made, and next steps to expedite resolution.
c. Review resolved Problems to confirm the root cause has been identified and the workaround has resolved the issue.
d. Review resolved known errors to confirm the implemented permanent solution has resolved the issue.
e. All Completed Problem records are validated for closure during the review meeting.

4.0 Change Management

This section outlines the interactions a partnering organization has with eHealth Ontario with regards to change management on any component that enables operation of an eHealth Ontario service. It details the steps needed to implement a change to technical components involved in successful delivery of eHealth Ontario services, according to the respective technical domains of responsibility for each organization involved.

The goal of Change Management is to minimize risk to the IT environment by ensuring that clear and standardized procedures are in place for the efficient and successful handling of all changes. A Change Request (CR) is required for all changes made to components that support a live eHealth Ontario service. A CR is a record containing the details of the change being requested, and includes start/end dates and times, the tasks to be performed, back-out procedures, and the resource(s) assigned, as defined by the eHealth Ontario Change Management process.

The information in this section is intended for both the eHealth Ontario Change Management team and the Change Management team within the partnering organization. It is also intended for eHealth Ontario's Client Services and Service Delivery personnel responsible for responding to partner inquiries regarding changes. The partnering organization is responsible to facilitate utilization of the change management touchpoints captured in this document with their change management team and any vendors or third party service providers having a direct relationship with them.

4.1 Change Management Criteria

Changes initiated by either eHealth Ontario or the partnering organization and impacting the eHealth Ontario service must be presented to eHealth Ontario's Change Approval Board (CAB). Changes include any addition, modification, or removal of any item that is part of the eHealth Ontario service. An item can include IT Services, Configuration Items, Processes, Documentation, etc.

eHealth Ontario requires seven business days' notice of changes to components that owned or managed by the partnering organization.

eHealth Ontario will provide partnering organizations with five business days' notice of changes to an eHealth Ontario service that may impact end users and/or components owned or managed by the partnering organization.

A change request (CR) for a live eHealth Ontario services is to be initiated by the partnering organization by contacting the eHealth Ontario Service Desk. The eHealth Ontario Service Desk then assigns support of the change request to either the Deployment Manager or Service Manager assigned to the eHealth Ontario Service. That Manager will then, with support from the partnering organization, document the partnering organization-initiated CR and will provide representation for the change at the eHealth Ontario CAB meetings.

The partnering organization will assign a representative to be the single point of contact (SPOC) for the eHealth Ontario Deployment Manager or Service Manager to work with after creation of a ticket through the eHealth Ontario Service Desk. The representative of the partnering organization will be responsible to obtain necessary change approvals and authorizations within the partnering organization prior to requesting the change.

Examples of changes include (but are not limited to):

- Infrastructure (including Portal and web-based services)
- Application
- Database
- Changes to standard operation process and/or procedures

4.2 Change Matrix

Below are eHealth Ontario change types and definitions. Partnering organizations must align with these definitions in order to utilize and trigger the eHealth Ontario Change Management process.

This terminology is used in the remainder of this section.

Change Type eHealth Ontario	Definition
Standard Change	A Change that is recurrent, low risk, low impact, follows a pre-defined path and for which approvals have been obtained in advance of implementation. This type of Change does not need to be reviewed by CAB.
Normal Change	A Change that must follow the entire Change Management process with final approval granted at CAB. The Change Management process includes assessment, authorization, CAB approval, and scheduling of the Change prior to implementation.
Emergency – Break/Fix Change	A Change that responds quickly to a critical interruption or eliminates a high risk of interruption and which requires immediate or expedited resolution. This type of Change is due to an incident and will normally have an expedited assessment and/or authorization procedure to minimize any risks of implementation.
Emergency – Business Change	A Change that responds quickly to an urgent client requirement where non-implementation will lead to a loss of reputation. This type of Change will normally have an expedited assessment and/or authorization procedure to minimize any risks to successful implementation.

Table 2 -Definition of Change Types

4.3 Scheduled CAB and Submission Deadline for Normal Changes

Below is the eHealth Ontario Change Advisory Board (CAB) schedule for reviewing and approving normal changes. A partnering organization must submit a CR to the assigned Service Manager by 12:00 p.m. Thursday which will then be reviewed by eHealth Ontario and submitted for the following Wednesday’s CAB agenda.

Organization	Date / Time	Submission Deadline
eHealth Ontario CAB*	Wednesday 10:00am – 12:00pm	Thursday 12:00pm

All Change Requests (CRs) submitted by a partnering organization for approval by the eHealth Ontario CAB must have cycled through proper authorization by designated officials from within the partnering organization. All responsibility for obtaining all necessary authorizations remain with the submitting party and eHealth Ontario assumes that such authorization has taken place upon receipt of the change request.

4.4 CAB Participation

The eHealth Ontario Service Manager or Deployment Manager represents the partnering organizations changes at the eHealth Ontario CAB. Representatives of the partnering organization do not attend eHealth Ontario CAB.

eHealth Ontario does not participate in the change approval processes of partnering organizations.

4.5 Maintenance Window

A maintenance window is a pre-defined period for implementing planned changes to components that support an eHealth Ontario service with minimal impact to interdependent components and the end users.

A maintenance window allows for proper planning of change activities, impact assessment, conflict assessment, and resourcing. It represents a period of low activity for most systems and services and is therefore an acceptable period to conduct maintenance and schedule changes with minimal impact to interdependent components and the end users.

The regular maintenance window for eHealth has been established, as follows:

Organization	Regular Maintenance Window
eHealth Ontario	Sunday 12:00 a.m. – 06:00 a.m.

A change can be scheduled outside of the Regular Maintenance Window in order to meet the business needs of the partnering organization. This must receive prior approval from the eHealth Ontario Service Owner.

eHealth Ontario will inform partnering organizations and impacted end user sites via the eHealth Ontario Service Desk when changes affect accessibility and availability of eHealth Ontario services using the communication of a Change Advisory. A Change Advisory is also known within eHealth Ontario as a *planned outage*.

4.6 Mandatory Change Information

The following information must be included in all Change Requests (CRs) submitted by the partnering organization:

- Change Reason
- Change Details
- Notification Required
- Is there a Disaster Recovery component to this change
- Does documentation (training manuals, build-books, etc.) exist
- Has this change has been successfully tested in the Infrastructure Lab

- Risk Level
- Impact
- Urgency
- Summary
- User Impact (If yes, identify impact in the user impact field).
- Outage Required (If yes or partial, identify the outage start/end dates).
- Impacted Areas Update
- Requested Start/End Dates
- Product Categorization (Tier 1 field)
- Link a Business Service (BSI) or an IT Service (ITS) Configuration Item (and the Components if applicable) using the CI name field
- Infrastructure Change Implementer

An accompanying implementation plan must be provided for every CR submitted by the partnering organization. The eHealth Ontario template for an implementation plan must be used. The partnering organization is to provide the necessary information to the eHealth Ontario Service Manager or Deployment Manager who completes the template on their behalf.

4.7 Change Freeze

A change freeze applies to Normal Changes in eHealth Ontario's live IT environments. A change freeze is established to minimize risks to environments and may be implemented by eHealth Ontario to support major project roll-outs, disaster recovery exercises, or major events that have the potential to heighten the overall risk of a change to public health (e.g., declared pandemic).

eHealth Ontario will advise the partnering organization no less than 30 calendar days in advance of a planned change freeze period. In all instances of a change freeze initiated by eHealth Ontario, an exemption process will be presented to the partnering organization with a Change Freeze Statement.

Partnering organizations who own or manage components that support successful operation of an eHealth Ontario service must inform eHealth Ontario via the eHealth Ontario Service Desk no less than 30 calendar days in advance of the planned change freeze period.

4.8 Escalation for Change Requests

Any issues encountered during implementation and provisioning of a change request are treated as a service incident. As such, they are addressed using the eHealth Ontario Incident Management process. Refer to the above Incident Management section of this document for details.

4.9 Change Lead Times

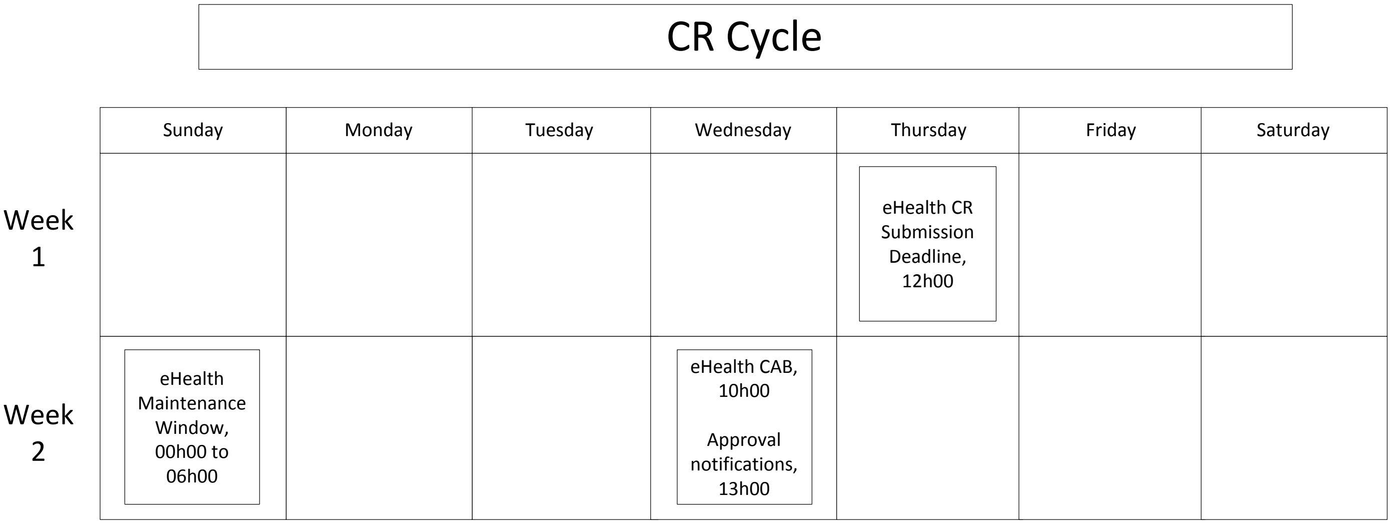
Business Impact or Potential Business Impact will be assessed by eHealth Ontario during an initial change review and CAB assessments.

The table below highlights the lead times required by eHealth Ontario for a change after a change request has been submitted to the eHealth Ontario Service Desk and reviewed by the assigned eHealth Ontario Deployment or Service Manager, and based on the perceived impact of the change.

Change Impact	Description	Change Implementation Lead Time Required
1-Extensive/Widespread	High-impact change with a major business impact or high visibility across the user base. • Results from a change made by operations or infrastructure (e.g., consolidating two application servers that result in complete failure of user availability). • Changes that are lengthy or for which back-out procedures are either lengthy or non-existent (e.g., updating database versions on the application server, major application release).	10 Business Days
2-Significant/Large	A medium/high-impact change that may have a major business impact or high visibility across the user base. The primary difference between medium/high and high-level impact change is that medium/high-impact changes may require involved back-outs but they can be backed out nonetheless.	10 Business Days
3-Moderate/Limited	Medium-impact changes with potentially minimal impact to the organization. Back–out procedures are relatively easy and effective.	5 Business Days
4-Minor/Localized	Low-impact changes are routine day-to-day changes or those which affect single customers / small groups. They are categorized and streamlined but are still tracked as part of change performance. Although service requests can be considered low-impact changes, IT operations groups must keep them separate for more effective management of resource utilization.	5 Business Days

Table 3 -Service Impact and Corresponding Change Lead Times

4.10 Change Request Timelines



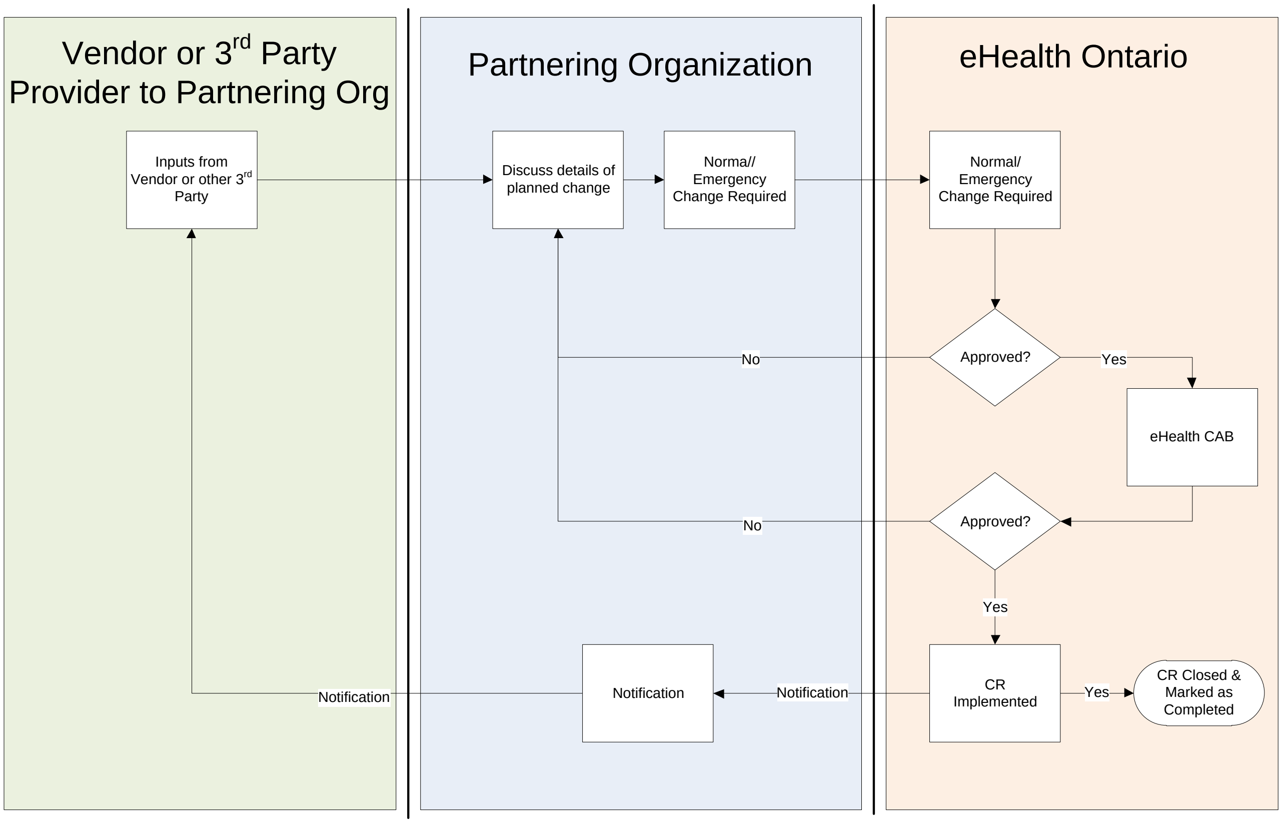
CR Cycle

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Week 1					eHealth CR Submission Deadline, 12h00		
Week 2	eHealth Maintenance Window, 00h00 to 06h00			eHealth CAB, 10h00 Approval notifications, 13h00			

Figure 6 - Change Request Submission and Approval Cycle

4.11 Normal and Emergency CR Process Flow

The diagram below depicts the process by which Normal and Emergency Changes will flow between eHealth Ontario and the partnering organization for the eHealth Ontario service.



Vendor or 3rd Party Provider to Partnering Org
Partnering Organization
eHealth Ontario
Inputs from Vendor or other 3rd Party
Discuss details of planned change
Norma// Emergency Change Required
Normal/ Emergency Change Required
Approved?
No
Yes
eHealth CAB
Approved?
No
Yes
CR Implemented
Yes
CR Closed & Marked as Completed
Notification
Notification
Notification

Figure 7 - Normal and Emergency Change Request Support Flow

4.12 Types of Changes

The following section presents detailed process steps for each type of change for an eHealth Ontario service, based on the partnering organization initiating the change request and the organization responsible for implementing the change.

4.12.1 Normal Change

4.12.1.1 Partnering Organization Initiated and eHealth Ontario Implemented

Initiator	Partnering Organization	**Implementer**	eHealth Ontario
Situation	Normal/planned changed with business impact It is assumed that the change has already been approved by the partnering organization's internal change authority.		
Submission deadline	Thursday 12:00 p.m. for implementation after eHealth Ontario's CAB meeting on the following Wednesday		
Steps	1. The partnering organization opens a service request with the eHealth Ontario Service Desk. 2. The assigned eHealth Ontario team, in collaboration with the partnering organization representative, creates the CR in the eHealth Ontario ITSM Tool before the submission deadline date and time. 3. The partnering organization representative receives a notification via email from the eHealth Ontario Service Manager or Deployment Manager of the eHealth Ontario change, requiring approval by the partnering organization. 4. The eHealth Service Manager or Deployment Manager discusses the list/impact of changes for eHealth Ontario's CAB approval with the partnering organization representative. 5. The eHealth Ontario Service Manager or Deployment Manager obtains approval for the CR at eHealth CAB, and informs the partnering organization. ➢ *Note: For any CR that is rejected by eHealth Ontario's CAB, the eHealth Ontario's Service Manager or Deployment Manager will provide the partnering organization representative with information on why the change was rejected.* 6. eHealth Ontario implements the change. 7. eHealth Ontario's Service Manager or Deployment Manager notifies the partnering organization representative of the status of implementation (i.e., successful / backed out / failed). 8. eHealth Ontario puts the CR into 'resolved' status.		

4.12.1.2 eHealth Ontario Initiated and eHealth Ontario Implemented

Initiator	eHealth Ontario	**Implementer**	eHealth Ontario
Situation	Normal/planned changed with impact or risk of impact to the eHealth Ontario service, supporting infrastructure, or process		
Submission deadline	Thursday 12:00 p.m. for implementation after eHealth Ontario's CAB meeting on the following Wednesday		
Steps	1. The eHealth Ontario team creates a CR. *2.* eHealth Ontario's Service Manager or Deployment Manager provides the partnering organization representative with details of the change before the eHealth Ontario Change submission deadline date and time. 3. The eHealth Ontario team responsible for the change obtains internal CAB approval. 4. eHealth Ontario's Service Manager or Deployment Manager informs the partnering organization representative that the CR was approved by eHealth Ontario's CAB. 5. eHealth Ontario implements the change. 6. eHealth Ontario's Service Manager or Deployment Manager notifies the partnering organization representative of the status of implementation (i.e., successful / backed out / failed). 7. eHealth Ontario puts the CR into 'resolved' status.		

4.12.1.3 Partnering Organization Initiated and Partnering Organization Implemented

Initiator	Partnering Organization	**Implementer**	Partnering Organization
Situation	Normal/planned changed with business impact		
Submission deadline	Not applicable		
Steps	1. Partnering organization Service Manager (or like role) advises the eHealth Ontario Service Desk of the normal change completion.		

4.12.2 Business Emergency

4.12.2.1 Partnering Organization and eHealth Ontario implemented

Initiator	Partnering Organization	**Implementer**	eHealth Ontario
Situation	System available but CR needs to be implemented without normal change process, i.e., business priority. It is assumed that the change has already been approved by the partnering organization's internal change authority.		
Submission deadline	Lead time for normal/planned change is not met		
Steps	1. eHealth Ontario team, in collaboration with the partnering organization representative, creates the business emergency CR. 2. eHealth Ontario's Service Manager or Deployment Manager follows the internal eHealth Ontario change process and obtains Emergency CAB (ECAB) authorization. ➢ *Note: For any CR that is rejected by eHealth Ontario's ECAB, the eHealth Ontario Service Manager* or Deployment Manager *will provide the partnering organization representative with information on why the change was rejected.* 3. eHealth Ontario's Service Manager or Deployment Manager informs the partnering organization representative of ECAB approval. 4. eHealth Ontario implements the change. 5. eHealth Ontario's Service Manager or Deployment Manager notifies the partnering organization of the status of implementation (i.e., successful / backed out / failed). 6. eHealth Ontario team places the CR into 'resolved' status.		

4.12.2.2 eHealth Ontario Initiated and eHealth Ontario Implemented

Initiator	eHealth Ontario	**Implementer**	eHealth Ontario
Situation	System available but CR needs to be implemented without normal change process, i.e., business priority		
Submission deadline	Lead time for normal/planned change is not met and can only be submitted during eHealth Ontario business hours		
Steps	1. The eHealth Ontario team creates a business emergency CR. 2. eHealth Ontario's Service Manager or Deployment Manager notifies and provides the partnering organization representative with details of the expedited change/business emergency. 3. eHealth Ontario's team follows the eHealth Business Emergency Change process to obtain approval. 4. eHealth Ontario implements the change. 5. eHealth Ontario's Service Manager or Deployment Manager notifies the partnering organization representative of the status of implementation (i.e., successful / backed out / failed). 6. eHealth Ontario places the CR into 'resolved' status.		

4.12.2.3 Partnering Organization Initiated and Partnering Organization Implemented

Initiator	Partnering Organization	**Implementer**	Partnering Organization
Situation	System available but CR needs to be implemented without normal change process, i.e., business priority.		
Submission deadline	Not applicable		
Steps	1. Partnering organization Service Manager (or like role) advises the eHealth Ontario Service Desk of the business emergency change completion.		

4.12.3 Break-fix Emergency Changes

4.12.3.1 Partnering Organization Initiated and eHealth Ontario Implemented

eHealth Ontario internal break-fix processes apply to this scenario, as documented here.

Initiator	Partnering Organization	**Implementer**	eHealth Ontario
Situation	Incident opened – Emergency break/fix change is submitted to Change Management. It is assumed that the change has already been approved by the partnering organization's internal change authority.		
Submission deadline	N/A		
Steps	1. The partnering organization representative notifies the eHealth Ontario Service Desk of the requested Change that is linked to a Priority 1 or 2 incident ticket. 2. eHealth Ontario follows the applicable internal Emergency change process, depending on the priority level, as follows: a. For a Priority 1 or 2 incidents, provided any latent CRs are filed within 24 hours. b. For a priority 3 or 4 incidents, provided an Emergency Break-fix change request is submitted for approval. 3. eHealth Ontario implements the change. 4. eHealth Ontario's Service Manager or Deployment Manager notifies the partnering organization representative of the status of implementation (i.e., successful / backed out / failed). 5. eHealth Ontario's change requestor places the emergency break-fix or latent CR into 'closed' status.		

4.12.3.2 eHealth Ontario Initiated and eHealth Ontario Implemented

eHealth Ontario internal break-fix and latent processes apply to this scenario, as documented here.

Initiator	eHealth Ontario	**Implementer**	eHealth Ontario
Situation	Priority 1 or Priority 2 Incident opened - system down (break/fix)		
Submission deadline	Not applicable		
Steps	1. The eHealth Ontario team implements the emergency change. 2. eHealth Ontario follows the applicable internal Emergency change process for a Priority 1 or 2 Incident including ensuring any latent CRs are filed within 24 hours. 3. eHealth Ontario implements the emergency change. 4. eHealth Ontario's Service Manager or Deployment Manager advises the partnering organization representative of the emergency change completion. 5. eHealth Ontario's change requestor places the associated or latent CR into 'resolved' status.		

4.12.3.3 Partnering Organization Initiated and Partnering Organization Implemented

Initiator	Partnering Organization	**Implementer**	Partnering Organization
Situation	Priority 1 or Priority 2 Incident (restoration) opened - system down (break/fix)		
Submission deadline	Not applicable		
Steps	1. The partnering organization's Service Manager (or like role) advises the eHealth Ontario representative of the emergency change completion.		

4.12.4 Standard Changes

Standard Changes are pre-approved by CAB for authorization and do not require either the partnering organization or eHealth Ontario CAB approval to proceed to implementation.

A change is qualified by CAB as a standard change when its implementation will not result in any downtime or degradation to the service performance that it is targeting and has no impact to other systems, components, or configuration items.

4.13 Service Environments

Implementation of change requests are evaluated and tested in lower environments prior to being implemented into the live Production environment of the eHealth Ontario service. However, partnering organizations are not involved in cycles through eHealth Ontario non-production or 'lower environments,' e.g., testing and pre-production.

After initiation of the change request by the partnering organization through the eHealth Ontario Service Desk, the Service Manager or Deployment Manager then represents the change request on behalf of the partnering organization in the following ways:

- Ushers CR through the promotion path of lower environments
- represents the CR at eHealth Ontario CAB
- tracks approval/promotion of the CR into the eHealth Ontario Production environment

Partnering Organizations should be aware that the eHealth Ontario Production environment is supported 7/24/365; non-production or ‘lower environments’ are supported during eHealth Ontario business hours from 8:00 a.m. to 5:00 p.m., EST.

5.0 Service Level Management

5.1 Service Availability

Service Availability is a critical part of overall performance reporting for an eHealth Ontario service. It is established based on the sum of availability of all individual components that enable successful performance of the service. Partnering organizations must provide to eHealth Ontario an operational availability target for components that they own or manage which enable performance of an eHealth Ontario service. This should be provided during the project phase of the service and eHealth Ontario should be informed of any changes to this target during the operational life of the service via the eHealth Ontario Service Desk.

eHealth standards for availability and affiliated service levels in support of targeted availability of an eHealth Ontario services are as follows:

Service Level Summary			
Service Level Component Metric	**Target Achievement Metrics**	**Measurement Criteria**	**Reporting Frequency**
Service Availability			
eHealth Ontario Service Availability - **Uptime**	Established individually for each eHealth Ontario Service – represented as a percentage (%) of Maximum Available Time per month	***Maximum Available Time*** is the agreed time (measured as total minutes per month) of service in the reporting period and is calculated as follows: *Availability* = Maximum Available Time – Unplanned Downtime / Maximum Available Time *100 ***Unplanned Downtime*** (measured in minutes) refers to service interruptions classified by eHealth Ontario as P1-Critical but excludes: • Planned downtime as a result of pre-approved maintenance • Interruptions occurring outside the agreed hours of support • Service interruptions classified by eHealth Ontario as P2-High or lower	Monthly
Disaster Recovery (DR)			
Recovery Time Objective (RTO)	Established individually for each eHealth Ontario	The recorded execution duration in which the IT service and its dependent services are recovered	As needed

Service Level Summary			
Service Level Component Metric	**Target Achievement Metrics**	**Measurement Criteria**	**Reporting Frequency**
	Service and/or function.	as a whole.	
Recovery Point Objective (RPO)	Established individually for each eHealth Ontario Service and/or function.	The recorded time period during which data might be lost from an IT service due to a major incident. RPO is independent of the time to restore the system (RTO).	As needed
SLAs			
eHealth Ontario Service – Incidents Mean Time to Resolve (MTTR)	eHealth Ontario Standard for Incidents	Incidents are assigned priority based on Impact and Scope (priority 1, 2, 3 and 4), with associated SLAs for resolution. The eHealth Ontario KPI for MTTR is to resolve 90% of all incident tickets (all priorities) within SLA.	Monthly
eHealth Ontario Service – Service Request Resolved within Target	eHealth Ontario Standard for Service Requests	The average length of time from the time a service request is recorded to the time it is fulfilled. Each priority has a different target time to resolve with an overall goal of achieving these resolutions times 90% of the time.	Monthly
Privacy Operations	eHealth Ontario Standard for Service Requests	The average length of time from the time a service request is recorded to the time it is fulfilled. Each priority has a different target time to resolve with an overall goal of achieving these resolutions times 90% of the time.	N/A
Privacy Incident and Breach Management	eHealth Ontario Standard for Incidents	The average length of time from the time an incident is recorded to the time it is resolved. Each priority has a different target time to resolve with an overall goal of achieving these resolutions times 90% of the time. The Incident Resolved within Target or IRT, with respect to all Incidents is measured by priority and represents the percentage of incidents where resolution occurs within the target achievement expectation.	N/A

Service Level Summary			
Service Level Component Metric	**Target Achievement Metrics**	**Measurement Criteria**	**Reporting Frequency**
Security Incident Management	eHealth Ontario Standard for Incidents	The average length of time from the time an incident is recorded to the time it is resolved. Each priority has a different target time to resolve with an overall goal of achieving these resolutions times 90% of the time. The Incident Resolved within Target or IRT, with respect to all Incidents is measured by priority and represents the percentage of incidents where resolution occurs within the target achievement expectation.	Monthly
eHealth Ontario Service Desk			
Call Answer Speed	Within 60 seconds 90% of the time	Time to answer a user's telephone call averaged over the month with a target of 90% of the calls being answered in 60 seconds.	Monthly
Abandonment Rate	< or = to 5% of total calls received	Number of callers who hang up before their call is answered as a percentage of the total calls answered. Measured over all clients to whom eHealth Ontario provides support services monthly. Calls to the e-Health Ontario Service Centre can be placed during business hours.	Monthly
Incidents reported via Email	Based on the standard eHealth Ontario Service Level Objective (SLO)	Within 2 Hours • 70% until April 31, 2016 • 75% from May 1 to September 30, 2016 • 80% post October 1, 2016 Within 8 Hours • 85% until April 31, 2016 • 90% from May 1 to September 30, 2016 • 98% post October 1, 2016	Monthly

Table 4 -Service Levels Summary

5.2 Service Review Meetings

A Service Review may be performed through established service review meetings at an agreed frequency (usually monthly). The meetings may be used to discuss service level targets, service availability, general concerns, and upcoming planned maintenance and changes being performed by both eHealth Ontario and the partnering organization. The meetings are facilitated by the eHealth Ontario Client Program Manager or Service Manager.

Appendix A - Statutory Holidays & eHealth Ontario Holidays

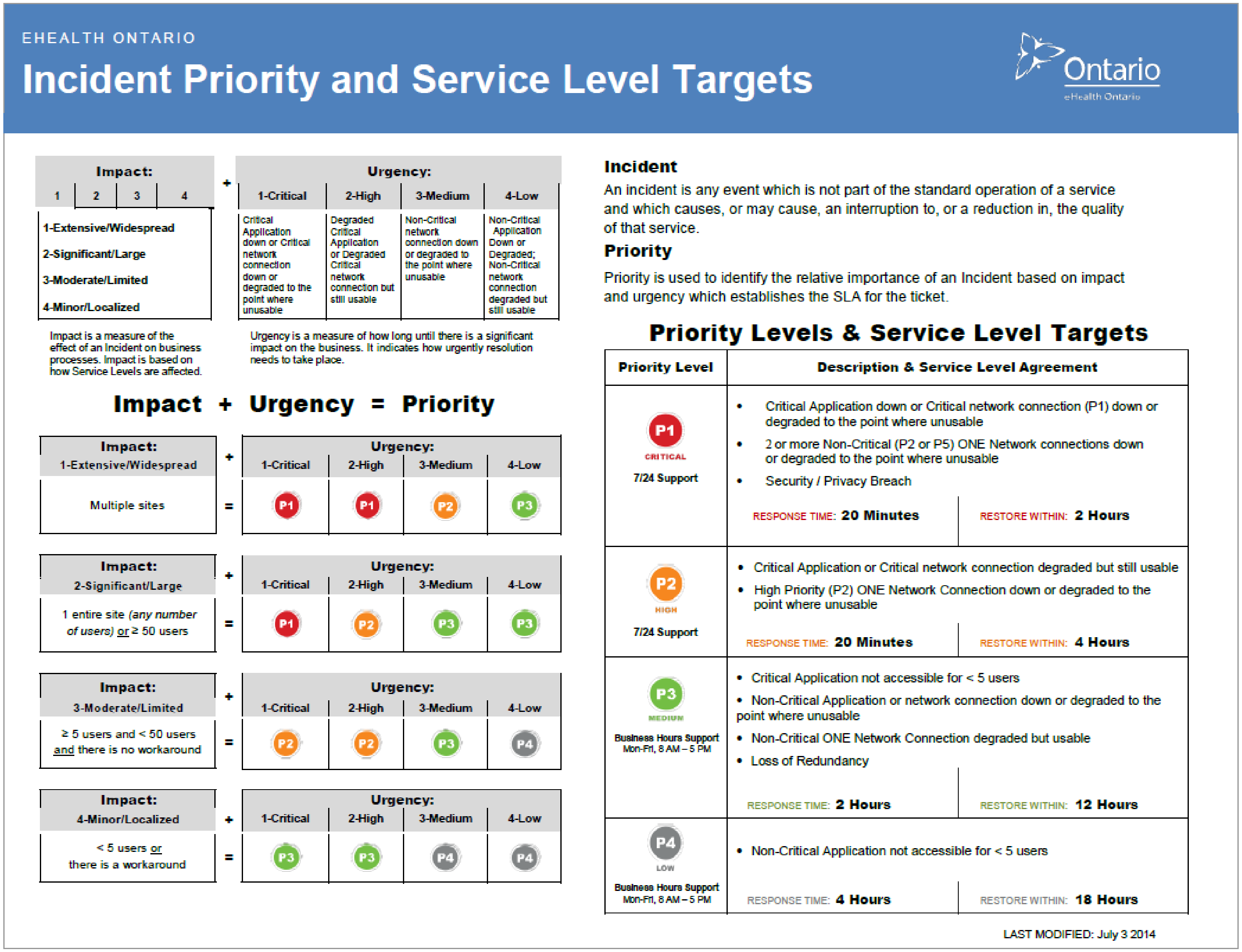
Listed below are the official statutory holidays observed in Ontario and additional days observed by eHealth Ontario. The SLA clock will be stopped on holidays observed by eHealth Ontario for incident resolution involving key actions from eHealth Ontario support teams that are designed to operate during business hours only.

Statutory Holiday	Province of Ontario
New Year's Day	Holiday
Family Day	Holiday
Good Friday	Holiday
Victoria Day	Holiday
Canada Day	Holiday
Labour Day	Holiday
Thanksgiving	Holiday
Christmas Day	Holiday
Boxing Day	Holiday

Non-statutory Holiday	eHealth Ontario
Easter Monday	Holiday
August Civic holiday (a.k.a., Simcoe Day)	Holiday
Remembrance Day	Holiday

Note: The actual date of these holidays changes from year to year, with the exception of Remembrance Day.

Appendix B - eHealth Standard Incident Priority and Service Level Targets



EHEALTH ONTARIO

Incident Priority and Service Level Targets

Ontario
eHealth Ontario

Impact:				+	Urgency:			
1	2	3	4		1-Critical	2-High	3-Medium	4-Low
1-Extensive/Widespread 2-Significant/Large 3-Moderate/Limited 4-Minor/Localized					Critical Application down or Critical network connection down or degraded to the point where unusable	Degraded Critical Application or Degraded Critical network connection but still usable	Non-Critical network connection down or degraded to the point where unusable	Non-Critical Application Down or Degraded; Non-Critical network connection degraded but still usable

Impact is a measure of the effect of an Incident on business processes. Impact is based on how Service Levels are affected.

Urgency is a measure of how long until there is a significant impact on the business. It indicates how urgently resolution needs to take place.

Impact + Urgency = Priority

Impact: 1-Extensive/Widespread	+	Urgency: 1-Critical	2-High	3-Medium	4-Low
Multiple sites	=	P1	P1	P2	P3

Impact: 2-Significant/Large	+	Urgency: 1-Critical	2-High	3-Medium	4-Low
1 entire site *(any number of users)* or ≥ 50 users	=	P1	P2	P3	P3

Impact: 3-Moderate/Limited	+	Urgency: 1-Critical	2-High	3-Medium	4-Low
≥ 5 users and < 50 users and there is no workaround	=	P2	P2	P3	P4

Impact: 4-Minor/Localized	+	Urgency: 1-Critical	2-High	3-Medium	4-Low
< 5 users or there is a workaround	=	P3	P3	P4	P4

Incident

An incident is any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.

Priority

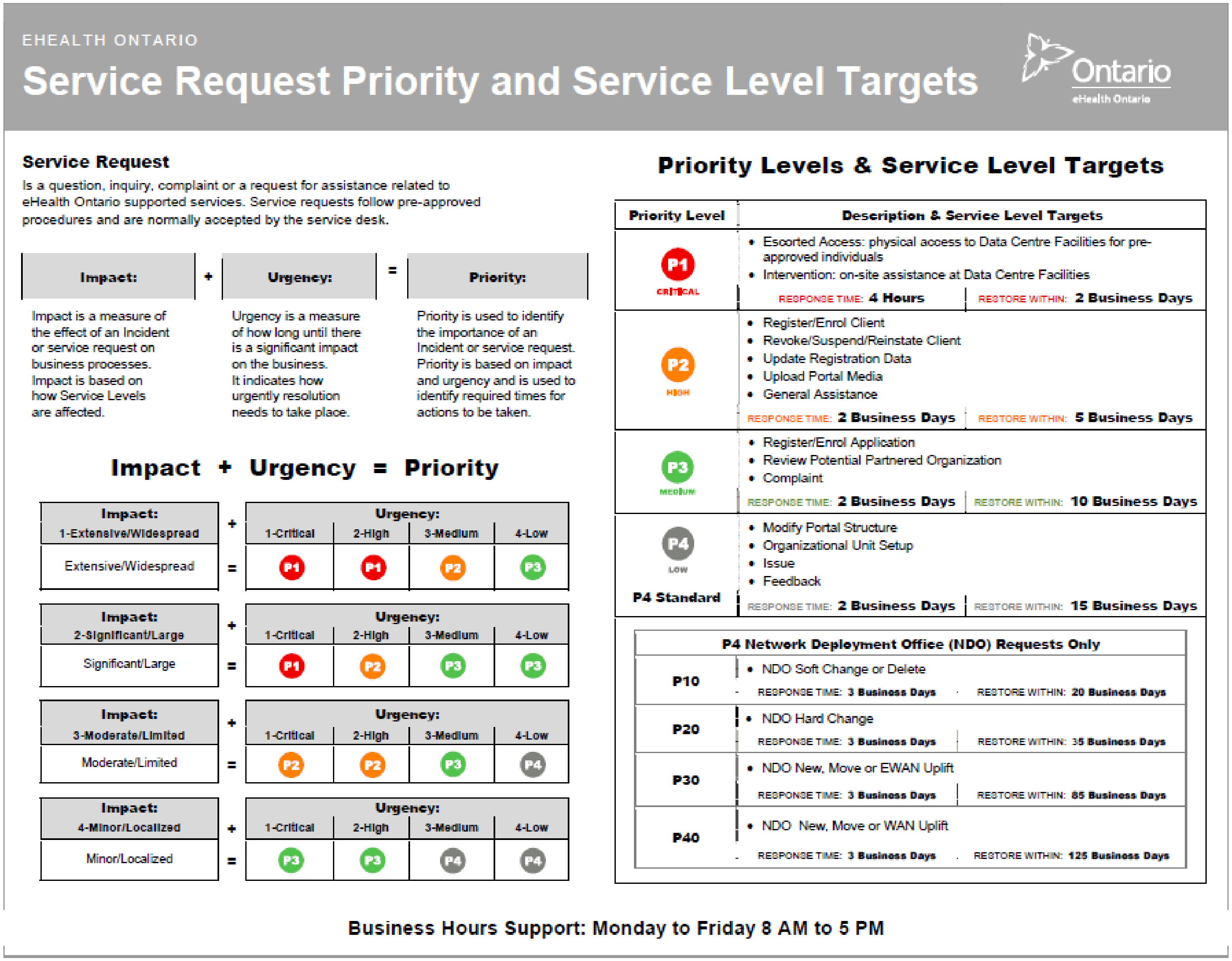
Priority is used to identify the relative importance of an Incident based on impact and urgency which establishes the SLA for the ticket.

Priority Levels & Service Level Targets

Priority Level	Description & Service Level Agreement	
P1 CRITICAL 7/24 Support	• Critical Application down or Critical network connection (P1) down or degraded to the point where unusable • 2 or more Non-Critical (P2 or P5) ONE Network connections down or degraded to the point where unusable • Security / Privacy Breach	
	RESPONSE TIME: **20 Minutes**	RESTORE WITHIN: **2 Hours**
P2 HIGH 7/24 Support	• Critical Application or Critical network connection degraded but still usable • High Priority (P2) ONE Network Connection down or degraded to the point where unusable	
	RESPONSE TIME: **20 Minutes**	RESTORE WITHIN: **4 Hours**
P3 MEDIUM Business Hours Support Mon-Fri, 8 AM – 5 PM	• Critical Application not accessible for < 5 users • Non-Critical Application or network connection down or degraded to the point where unusable • Non-Critical ONE Network Connection degraded but usable • Loss of Redundancy	
	RESPONSE TIME: **2 Hours**	RESTORE WITHIN: **12 Hours**
P4 LOW Business Hours Support Mon-Fri, 8 AM – 5 PM	• Non-Critical Application not accessible for < 5 users	
	RESPONSE TIME: **4 Hours**	RESTORE WITHIN: **18 Hours**

LAST MODIFIED: July 3 2014

Appendix C - eHealth Standard Service Request Priority and Service Level Targets



EHEALTH ONTARIO

Service Request Priority and Service Level Targets

Ontario
eHealth Ontario

Service Request

Is a question, inquiry, complaint or a request for assistance related to eHealth Ontario supported services. Service requests follow pre-approved procedures and are normally accepted by the service desk.

Impact:	+	Urgency:	=	Priority:
Impact is a measure of the effect of an Incident or service request on business processes. Impact is based on how Service Levels are affected.		Urgency is a measure of how long until there is a significant impact on the business. It indicates how urgently resolution needs to take place.		Priority is used to identify the importance of an Incident or service request. Priority is based on impact and urgency and is used to identify required times for actions to be taken.

Impact + Urgency = Priority

Impact:	+	Urgency:			
1-Extensive/Widespread		1-Critical	2-High	3-Medium	4-Low
Extensive/Widespread	=	P1	P1	P2	P3

Impact:	+	Urgency:			
2-Significant/Large		1-Critical	2-High	3-Medium	4-Low
Significant/Large	=	P1	P2	P3	P3

Impact:	+	Urgency:			
3-Moderate/Limited		1-Critical	2-High	3-Medium	4-Low
Moderate/Limited	=	P2	P2	P3	P4

Impact:	+	Urgency:			
4-Minor/Localized		1-Critical	2-High	3-Medium	4-Low
Minor/Localized	=	P3	P3	P4	P4

Priority Levels & Service Level Targets

Priority Level	Description & Service Level Targets	
P1 CRITICAL	• Escorted Access: physical access to Data Centre Facilities for pre-approved individuals • Intervention: on-site assistance at Data Centre Facilities	
	RESPONSE TIME: **4 Hours**	RESTORE WITHIN: **2 Business Days**
P2 HIGH	• Register/Enrol Client • Revoke/Suspend/Reinstate Client • Update Registration Data • Upload Portal Media • General Assistance	
	RESPONSE TIME: **2 Business Days**	RESTORE WITHIN: **5 Business Days**
P3 MEDIUM	• Register/Enrol Application • Review Potential Partnered Organization • Complaint	
	RESPONSE TIME: **2 Business Days**	RESTORE WITHIN: **10 Business Days**
P4 LOW	• Modify Portal Structure • Organizational Unit Setup • Issue • Feedback	
P4 Standard	RESPONSE TIME: **2 Business Days**	RESTORE WITHIN: **15 Business Days**

P4 Network Deployment Office (NDO) Requests Only		
P10	• NDO Soft Change or Delete	
	RESPONSE TIME: **3 Business Days**	RESTORE WITHIN: **20 Business Days**
P20	• NDO Hard Change	
	RESPONSE TIME: **3 Business Days**	RESTORE WITHIN: **35 Business Days**
P30	• NDO New, Move or EWAN Uplift	
	RESPONSE TIME: **3 Business Days**	RESTORE WITHIN: **85 Business Days**
P40	• NDO New, Move or WAN Uplift	
	RESPONSE TIME: **3 Business Days**	RESTORE WITHIN: **125 Business Days**

Business Hours Support: Monday to Friday 8 AM to 5 PM

Appendix D - Glossary of Acronyms

Term	Definition/Description
CAB	Change Advisory Board
CD	Consent Directive
CDM	Client Delivery Manager
CR	Change Request
DHDR	Digital Health Drug Repository
DI	Diagnotic Image
DPV	Drug Profile Viewer
ECAB	Emergency Change Advisory Board
ECR	Emergency Change Request
ERS	Enterprise Reporting System
HSC	Ministry of Health and Long-term Care Health Services Cluster
IMSP	Information Management Strategy and Policy Branch
ITIL	Information Technology Infrastructure Library. ITIL V3 is the version published in 2007, a.k.a. ITIL 2007 edition.
ITSM	Information Technology Service Management
Lower environments	Also known as, non-production environments. This refers to development environments (Development and Integration Testing (DIT)), testing environments (ITE1 and ITE2), and pre-production environments (PPE, PST (Partner Self-test), PHI testing).
MOHLTC APO	Ministry of Health and Long-term Care Access and Privacy Office
OLIS	Ontario Laboratories Information System
OPDP	Ontario Public Drug Programs (OPDP)
P1	Highest level Priority 1 (incident or ticket) - Critical
P2	Second highest Priority 2 (incident or ticket) - High
PHI	Personal Health Information
PI	Personal Information
Production environment	The environment where the eHealth Ontario service is live and made available to external users; it is the backbone of the operational life of the service.
PBM	eHealth Ontario Privacy Breach Management
SIM	eHealth Ontario Security Incident Management

Term	Definition/Description
SPOC	Single Point of Contact